



# ***GE Fanuc Automation***

---

***Programmable Control Products***

***PACSystems™  
Hot Standby CPU Redundancy***

***User's Guide***

*GFK-2308*

*June 2004*

## *Warnings, Cautions, and Notes as Used in this Publication*

### **Warning**

**Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.**

**In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.**

### **Caution**

**Caution notices are used where equipment might be damaged if care is not taken.**

**Note:** Notes merely call attention to information that is especially significant to understanding and operating the equipment.

This document is based on information available at the time of its publication. While efforts have been made to be accurate, the information contained herein does not purport to cover all details or variations in hardware or software, nor to provide for every possible contingency in connection with installation, operation, or maintenance. Features may be described herein which are not present in all hardware and software systems. GE Fanuc Automation assumes no obligation of notice to holders of this document with respect to changes subsequently made.

GE Fanuc Automation makes no representation or warranty, expressed, implied, or statutory with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of the information contained herein. No warranties of merchantability or fitness for purpose shall apply.

The following are trademarks of GE Fanuc Automation North America, Inc.

Alarm Master	Genius	PowerMotion	Series Six
CIMPLICITY	Helpmate	PowerTRAC	Series Three
CIMPLICITY 90-ADS	Logicmaster	ProLoop	VersaMax
CIMSTAR	Modelmaster	PROMACRO	VersaPoint
Field Control	Motion Mate	Series Five	VersaPro
GENet	PACSystems	Series 90	VuMaster
		Series One	Workmaster

<b>Introduction .....</b>	<b>1-1</b>
<b>Hot Standby CPU Redundancy.....</b>	<b>1-1</b>
Definitions.....	1-2
Features of Hot Standby CPU Redundancy .....	1-3
HSB Control Strategy.....	1-3
<b>Genius Hot Standby Operation.....</b>	<b>1-4</b>
Genius Output Control .....	1-4
<b>Online Programming.....</b>	<b>1-5</b>
<b>On-Line Repair.....</b>	<b>1-5</b>
<b>Related Publications.....</b>	<b>1-5</b>
 <b>System Configuration .....</b>	 <b>2-1</b>
<b>Components of a Hot Standby Redundancy System.....</b>	<b>2-1</b>
System Racks .....	2-1
Redundancy CPU Module.....	2-2
Redundancy CPUs Compared to Other PACSystems CPUs .....	2-2
Using the Redundancy CPU for Non-redundant Operation .....	2-3
Redundancy Memory Xchange Module .....	2-3
Redundant I/O System.....	2-4
Genius Bus Controller and Genius Devices .....	2-4
<b>Basic CPU Redundancy Setups Using Genius I/O .....</b>	<b>2-5</b>
Single Bus Networks .....	2-5
Hardware Configuration for Single Bus Networks .....	2-6
Dual Bus Networks.....	2-7
Hardware Configuration for Dual Bus Network .....	2-8
Location of GBCs and Blocks .....	2-8
Duplex Genius Output Mode.....	2-9
<b>Local I/O .....</b>	<b>2-9</b>
 <b>Configuration Requirements .....</b>	 <b>0-1</b>
<b>Using the Redundancy Wizards .....</b>	<b>3-2</b>
Synchronizing the Hardware Configurations.....	3-3
<b>Configuration Parameters .....</b>	<b>3-4</b>
CPU Parameters .....	3-4
Settings.....	3-4
Scan Parameters .....	3-5
Communications Window Considerations .....	3-5
Fault Parameters .....	3-6
Redundancy Parameters.....	3-7
Transfer List.....	3-8
Redundancy Memory Xchange Modules .....	3-10
Ethernet Interface.....	3-11
Rack Module Configuration Parameters .....	3-12

Bus Controller Configuration Parameters .....	3-12
Genius Device Configuration Parameters.....	3-12
<b>Storing (Downloading) Hardware Configuration .....</b>	<b>3-13</b>
<b>Configuring the Redundancy CPU for Non-redundant Operation .....</b>	<b>3-13</b>
<b>Operation .....</b>	<b>4-1</b>
<b>Powerup of a Redundancy CPU .....</b>	<b>4-2</b>
<b>Synchronization of the Time of Day Clocks .....</b>	<b>4-2</b>
<b>Synchronizing Redundant CPUs .....</b>	<b>4-3</b>
Dual Synchronization .....	4-3
Resynchronization.....	4-3
<b>HSB Control Strategy .....</b>	<b>4-4</b>
<b>%S References for CPU Redundancy .....</b>	<b>4-5</b>
<b>Scan Synchronization.....</b>	<b>4-6</b>
<b>Fail Wait Time .....</b>	<b>4-6</b>
<b>Data Transfer .....</b>	<b>4-7</b>
Input Data and Synchronization Data Transfer to the Backup Unit .....	4-7
Sweep Time Synchronization .....	4-7
Transition Contacts and Coils.....	4-7
Output Data Transfer to the Backup Unit.....	4-7
Data Transfer Time .....	4-8
Programming a Data Transfer from Backup Unit to Active Unit .....	4-9
Disabling Data Transfer Copy in Backup Unit (SVC_REQ #43).....	4-11
Command Block for SVC_REQ #43.....	4-12
Backup Qualification with SVC_REQ #43 .....	4-13
Validating the Backup PLC's Input Scan .....	4-13
Validating the Backup PLC's Logic Solution.....	4-13
<b>Switching Control to the Backup Unit .....</b>	<b>4-14</b>
Switching Times .....	4-14
Commanding a Role Switch from the Application Program (SVC_REQ #26) .....	4-14
Implementing Preferred Master Using SVC_REQ #26 .....	4-15
<b>RUN Disabled Mode .....</b>	<b>4-16</b>
<b>Error Checking and Correction.....</b>	<b>4-16</b>
<b>Timer and PID Functions.....</b>	<b>4-17</b>
<b>Timed Contacts .....</b>	<b>4-17</b>
<b>Multiple I/O Scan Sets.....</b>	<b>4-17</b>
<b>STOP to RUN Mode Transition .....</b>	<b>4-18</b>
<b>Genius Bus Controller Switching.....</b>	<b>4-18</b>
<b>Redundant IP Addresses.....</b>	<b>4-19</b>
<b>Ethernet Global Data in a Redundancy CPU .....</b>	<b>4-21</b>
Ethernet Global Data Production .....	4-21
Ethernet Global Data Consumption .....	4-21

<b>Fault Detection .....</b>	<b>5-1</b>
<b>Fault Detection .....</b>	<b>5-1</b>
<b>PLC Fault Table Messages for Redundancy .....</b>	<b>5-2</b>
Redundancy Fault Group (138).....	5-2
Other Fault Groups .....	5-4
<b>Fault Response .....</b>	<b>5-5</b>
<b>Redundancy Link Failures .....</b>	<b>5-6</b>
Redundancy Memory Xchange Module Hardware Failure .....	5-6
Redundancy Link Communications Failures.....	5-6
<b>Fault Actions in a CPU Redundancy System .....</b>	<b>5-7</b>
Configuration of Fault Actions .....	5-7
Configurable Fault Groups .....	5-7
Non-Configurable Fault Groups .....	5-9
Fatal Faults on Both Units in the Same Sweep .....	5-9
<b>Online Repair .....</b>	<b>5-10</b>
On-Line Repair Recommendations.....	5-10
Online Repair of the Genius Bus.....	5-10
Single Bus Networks.....	5-10
Dual Bus Networks .....	5-10
<b>Converting a Series 90-70 Redundancy System to PACSystems .....</b>	<b>6-1</b>
<b>Control Strategy Conversion .....</b>	<b>6-1</b>
<b>Applications with a Programmable Coprocessor Module .....</b>	<b>6-2</b>

This manual is a reference to the hardware components, configuration, programming and operation of Hot Standby CPU redundancy for the PACSystems RX7i. The information in this manual is intended to supplement the system installation, programming, and configuration information contained in the manuals listed under “Related Publications” on page 1-5.

### ***Hot Standby CPU Redundancy***

Hot Standby CPU Redundancy allows a critical application or process to continue operating if a failure occurs in any single component. A Hot Standby system uses two CPUs, an active unit that actively controls the process, and a backup unit that is synchronized with the active unit and can take over the process should it become necessary. The two units are synchronized when both are in Run Mode, the backup unit has received the latest status and synchronization information from the active unit via a redundant link, and both are running their logic solution in parallel.

Each unit must have a redundancy CPU (IC698CRE020) and one or two Redundancy Memory Xchange (IC698RMX016) modules. The redundancy communication paths are provided by one or two pairs of RMX modules.

Control automatically switches to the backup unit when a failure is detected in the active unit. You can initiate a switch of control by activating a toggle switch on the RMX module or activating a service request in the application program. When a user-initiated switch of control occurs, the CPUs switch roles; the active unit becomes the backup unit and the backup unit becomes active.

The system runs synchronously with a transfer of all control data that defines machine status and any internal data needed to keep the two CPUs operating in sync. The transfer of data from the active unit to the backup unit occurs twice per sweep. These CPU-to-CPU transfers are checked for data integrity.

## Definitions

<b>Redundancy</b>	The use of multiple elements controlling the same process to provide alternate functional channels in case of failure.
<b>CPU Redundancy</b>	A system with two PLC CPU units cooperating to control the same process.
<b>Critical Component</b>	Components that acquire or distribute I/O data or that are involved in execution of the control logic solution.
<b>Hot Standby</b>	A system where the backup (standby) unit is designated <i>before</i> any critical component failure takes place, and any necessary state/control information is passed to this designated backup unit so that it can take control <i>quickly</i> in the event of a critical component failure.
<b>Primary Unit</b>	The preferred unit to control the process in a Redundancy System. For redundant Genius I/O, the Genius Bus Controllers in the primary unit are configured for serial bus address 31.
<b>Secondary Unit</b>	The unit configured to control the process in a Redundancy System when the primary unit is unavailable or otherwise marked as not controlling the process. For redundant Genius I/O, the Genius Bus Controllers in the secondary unit are configured for serial bus address 30.
<b>Active Unit</b>	The unit that is currently controlling the process.
<b>Backup Unit</b>	The unit that is synchronized with the active unit and able to take over the process.
<b>Role Switch</b>	User-initiated switch of control, where the active unit becomes the backup unit and the backup unit becomes the active unit.
<b>Redundancy Link</b>	A complete communications path between the two CPUs, consisting of one RMX in the primary unit, one RMX in the secondary unit, and a high-speed fiber optic cable connecting them to each other.
<b>Synchronized</b>	Condition where both units are in Run Mode and the backup unit has received the latest status and synchronization information from the active unit via a redundancy link. When the two units are synchronized, they run their logic solution in parallel.
<b>Genius Hot Standby</b>	A feature of Genius devices whereby the device prefers output data from the Bus Controller at Serial Bus Address 31. When outputs from that Bus Controller are not available, the device takes output data from the Bus Controller at Serial Bus Address 30. If outputs from neither Controller are available, the device places its outputs in the designated default state.
<b>Genius Dual Bus</b>	The use of two Genius busses to control the same I/O devices. The busses are linked to the I/O devices by one or more Bus Switching Modules (BSMs). A BSM will automatically switch to the other bus if the active bus has a failure.

---

## Features of Hot Standby CPU Redundancy

- Survives any one single point of failure (excluding failures of Genius devices and bus stubs)
- Bumpless switching
  - *Synchronized* CPUs
  - One scan switching
  - Configurable transfer data size up to 2Mbytes
- Supports two redundancy communications links
- Online repair of failed component
- Online programming
- Redundancy Memory Xchange Module
  - Manual toggle switch for switching control between active and backup units
  - Five redundancy status LEDs (Link OK, Local Ready, Local Active, Remote Ready, Remote Active)
- Redundancy status bits and message logging
- Application-initiated role switching
- 10 Mbytes of user flash memory
- Memory Error Checking and Correction (ECC single bit correcting and multiple bit checking)
- Supports single and dual Genius bus networks
- Background diagnostics

## HSB Control Strategy

The HSB control strategy has the following characteristics:

- Active unit does not automatically switch to primary on resynchronization
- Critical control data plus all redundant outputs must be included in the output data transfer
- Bumpless switchover from active unit to backup unit
- Supports multiple dual bus Genius networks with redundant bus controllers in each synchronized PLC
- Supports multiple single bus Genius networks with a redundant bus controller in each synchronized PLC
- Supports multiple local Genius networks with single or dual busses, and single or dual bus controllers

## Genius Hot Standby Operation

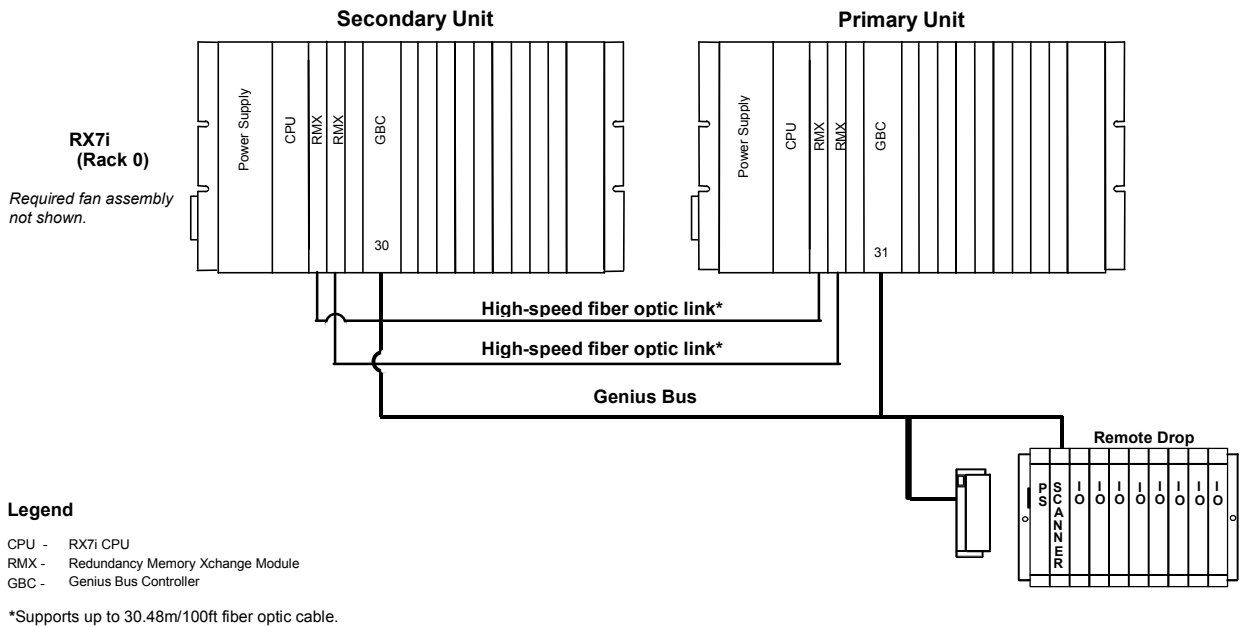
In a Hot Standby CPU redundancy system, the Genius outputs are controlled by only one unit (the active unit). The inputs are shared between both units. One unit is the Primary unit and the other is the Secondary unit. The Primary unit contains all externally redundant Genius Bus Controllers at Serial Bus Address 31; the Secondary unit contains all externally redundant Genius Bus Controllers at Serial Bus Address 30.

The Genius output devices are normally configured for Genius Hot Standby redundant operation. With this configuration, the devices choose between outputs from the Genius Bus Controller at serial bus address 31 and the Genius Bus Controller at serial bus address 30. If outputs from both Genius Bus Controllers are available, the devices will use outputs from bus address 31. If there are no outputs from bus address 31 for three consecutive Genius I/O bus scans, the devices will use the outputs from bus address 30. If outputs are not available from either bus address 31 or 30, the outputs go to their configured default (OFF or hold last state).

## Genius Output Control

In a Hot Standby CPU Redundancy system, the active unit determines the values of the Genius outputs.

Both the primary and secondary units send outputs regardless of which one is active. The user is responsible for ensuring that all redundant Genius outputs are included in the output data transfer. Because the same output values will then be sent to the GBCs in both units, the devices will receive the same output values from SBA 31 and SBA 30. There is no data interruption on switchover because both units are always sending Genius outputs.



---

## ***Online Programming***

On-line changes to the application program are permitted in both the active unit and the backup unit. The programming device must be connected to the unit in which changes are to be made in order to make any on-line changes.

## ***On-Line Repair***

A Hot Standby CPU Redundancy system permits online repair of failed components without disrupting the control application. A failed component can be replaced in either unit after first removing power from the rack in which it is installed.

After replacing the failed component, returning power to the rack, and placing the CPU in Run mode, the repaired unit synchronizes with the currently active unit. Upon successful synchronization, the repaired unit becomes the backup unit.

Online repair is described in more detail in chapter 5.

## ***Related Publications***

*PACSystems CPU Reference Manual*, GFK-2222

*PACSystems RX7i Installation Manual*, GFK-2223

*PACSystems RX7i Memory Exchange Modules*, GFK-2300

*TCP/IP Ethernet Communications for PACSystems*, GFK-2224

*PACSystems RX7i User's Guide to Integration of VME Modules*, GFK-2235

*CIMPLICITY Machine Edition Logic Developer-PLC Getting Started*, GFK-1918

*Series 90-70 Genius Bus Controller User's Manual*, GFK-2017

*Genius I/O System User's Manual*, GEK-90486-1

*Genius Discrete and Analog Blocks User's Manual*, GEK-90486-2

For the most recent versions of PACSystems and related documentation, visit the GE Fanuc website: <http://www.gefanuc.com/>.

# Chapter 2

## System Configuration

---

---

This chapter describes the hardware components for a Hot Standby CPU Redundancy system and describes system configurations for the basic redundancy schemes supported by PACSystems RX7i.

For detailed installation instructions for the RX7i, refer to the *PACSystems RX7i Installation Manual*, GFK-2223.

### ***Components of a Hot Standby Redundancy System***

- System Racks
  - Redundancy CPU
  - Redundancy Memory Xchange modules
  - Redundant I/O System
- Genius Bus Controller and Genius Devices

### **System Racks**

The following racks may be used as the CPU rack also referred to as Rack 0.

- IC698CHS017, 18 slot rear mount – Wall mount
- IC698CHS117, 18 slot front mount – Rack mount

The following Series 90-70 racks may be used as expansion racks in a Hot Standby CPU Redundancy System:

- IC697CHS750, 5-slot rear mount - standard rack
- IC697CHS790, 9-slot rear mount - standard rack
- IC697CHS791, 9-slot front mount - standard rack

## Redundancy CPU Module

To use the features described in this manual, a Redundancy CPU Module (IC698CRE020) must be installed in rack 0, slot 1 of both the primary and secondary units.

**Note:** An IC698CPE020 can be easily converted to a CRE020 by installing different firmware and moving a jumper. Detailed instructions are included in the firmware upgrade kit for CRE020.

The IC698CRE020 has 10MB of battery-backed RAM and 10MB of flash memory. It provides configurable reference memory limits for %AI (Analog Input), %AQ (Analog Output), %R (Register), and %W (bulk memory area) reference memory, as well as symbolic discrete reference memory and symbolic non-discrete reference memory.

Operation of this module can be controlled by the three-position RUN/STOP switch or remotely by an attached programmer and programming software. Program and configuration data can be locked through software passwords. The five CPU LEDs on the front of the module indicate the status of the CPU. Seven LEDs indicate the status of the Ethernet interface.

The IC698CRE020 has two configurable ports: COM 1 (RS-232) and COM2 (RS-485). The embedded Ethernet interface board controls two 10 BASE T/100 BASE TX ports and a configurable Station Manager (RS-232) port.

The IC698CRE020 supports the following Ethernet interface features:

- Redundant IP address
- PLC data monitoring over the web. Supports a combined total of up to 16 web server and FTP connections.
- Up to 255 Ethernet Global Data (EGD) exchanges with up to 100 variables per exchange.
- EGD upload and selective consumption of EGD exchanges.
- Upload and download of an Advanced User Parameter (AUP) file, which contains user customizations to internal Ethernet operating parameters.

### Redundancy CPUs Compared to Other PACSystems CPUs

The following features are not available:

- I/O and module interrupts: This includes the single edge triggered interrupts from the discrete input modules, the high alarm and low alarm interrupts from the analog input modules, and interrupts from VME modules. A program that declares I/O Interrupt triggers cannot be stored to a Redundancy CPU.
- 14-point interrupt module (IC697MDL671) is not supported[G11]
- Interrupt Blocks (I/O, timed, module): Logic that contains interrupt blocks cannot be stored to the CPU.
- VME integrator racks are not supported.
- Stop I/O Scan mode: If an attempt is made to place the PLC in this mode, the PLC will reject the selection and return an error.
- #OVR\_PRE %S reference, which indicates whether one or more overrides are active, is not supported and should not be used.

The following features operate differently with the CRE020 than they do with other PACSystems CPUs:

- Error checking and correction (ECC) is enabled.
- RUN/DISABLED mode. This is explained in chapter 4, Operation.
- User-configurable fault actions are not used when the CPUs are synchronized.
- STOP to RUN mode transition. For details, see “Synchronizing Redundant CPUs” in chapter 4.
- Background Window Timer (in Normal Sweep mode) default is 5ms
- Ethernet Global Data (EGD) is only produced by the active unit.

Also, be aware that instance data associated with IEC transitionals (PTCOIL, NTCOIL, PTCON, and NTCON) are not synchronized between the two CPUs. For details, refer to “Data Transfer” in chapter 4.

### Using the Redundancy CPU for Non-redundant Operation

The Redundancy CPU can be used for both redundant and non-redundant applications. The functionality and performance of a Redundancy CPU configured for non-redundant operation is the same as for a unit that is configured for redundant operation with no backup available. This includes the redundancy informational messages such as those generated when a unit goes to Run mode. Refer to Chapter 3, “Configuring the Redundancy CPU for Non-redundant Operation.”

### Redundancy Memory Xchange Module

The RMX modules provide a path for transferring data between the two redundancy CPUs. A complete communications path consists of one RMX in the primary unit, one RMX in the secondary unit, and two high-speed fiber optic cables connecting them to each other. This must be a two-node ring: no other reflective memory nodes are allowed to be part of this fiber optic network. The maximum cable length supported for a redundancy link is 30.48 meters/100 feet.

GE Fanuc **strongly recommends** two redundancy links (for a total of four RMX modules) be configured and installed. Optionally, systems can be configured for a single redundancy link (for a total of two RMX modules).

**Note:** It is recommended that the RMX modules be installed in slots 3 and 4 of the main rack. This gives VME interrupt request priority to the RMX modules. Although this configuration is recommended, it is not required that the RMX modules be located in slots 3 and 4.

The RMX module has a toggle switch that can be used to manually request a role switch. Eight LEDs, described on the next page, provide indication of module status.

**LEDs**

<b>LED Label</b>	<b>Description</b>
OK	ON indicates the module is functioning properly.
LINK OK	When used as a redundancy link (RMX only), ON indicates the link is functioning properly.
LOCAL READY	ON indicates the local unit is ready.
LOCAL ACTIVE	ON indicates the local unit is active.
REMOTE READY	ON indicates the remote unit is ready.
REMOTE ACTIVE	ON indicates the remote unit is active.
OWN DATA	ON indicates the module has received its own data packet from the network at least once.
SIGNAL DETECT	ON indicates the receiver is detecting a fiber optic signal.

## Redundant I/O System

### Genius Bus Controller and Genius Devices

The Genius Bus Controller (IC697BEM731) interfaces the RX7i to a Genius I/O bus. The bus controller scans Genius devices asynchronously and exchanges I/O data with the CPU.

A Hot Standby CPU Redundancy system can have multiple Genius I/O bus networks. Any Genius device can be placed on the bus (Genius blocks, Field Control, Remote I/O Scanner, VersaMax I/O, etc.). The Genius outputs are determined by the active unit. The Genius Bus Controller in the primary unit has a Serial Bus Address of 31; the Genius Bus Controller in the secondary unit has a Serial Bus Address of 30.

## Basic CPU Redundancy Setups Using Genius I/O

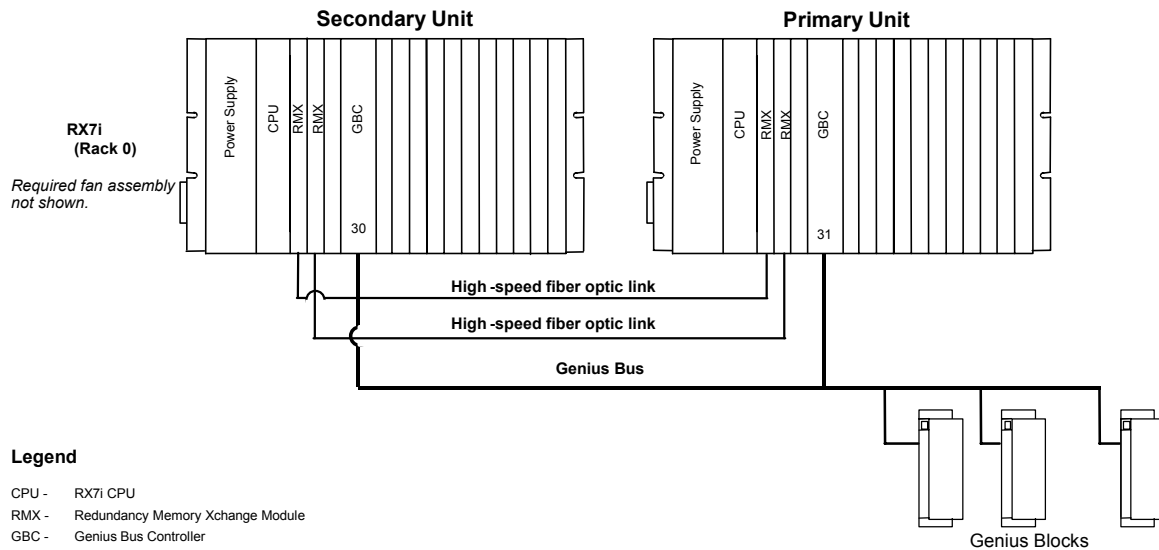
Hot Standby CPU Redundancy supports two types of bus schemes for the Genius networks:

- Single bus networks
- Dual bus networks

PACSystems CPU Redundancy implements a floating master algorithm. If an application requires a preferred master algorithm, see “Implementing Preferred Master” in chapter 4.

### Single Bus Networks

This type of network uses a single bus with one Genius bus controller in each PLC.



The single bus setup is suitable if the application does not require redundant I/O busses.

When using single-bus Genius networks in a Hot Standby CPU Redundancy system, one Genius Bus Controller for the bus must be located in the primary unit and one in the secondary unit. There can be multiple Genius buses in the system. The bus controllers in the primary unit are assigned Serial Bus Address 31. The bus controllers in the secondary unit are assigned Serial Bus Address 30.

Genius output devices will use outputs from Serial bus Address 31 in preference to outputs from Serial bus Address 30. Outputs are determined by the active unit, regardless of which bus controller provides the outputs since all redundant Genius outputs are transferred from the active unit to the backup unit.

Any type of Genius device can be connected to the network. Each Genius network can have up to 30 additional Genius devices connected to it. You may want to reserve one Serial Bus Address for the Hand-Held Monitor.

As a safety feature, a watchdog timer protects each Genius I/O link. The bus controller periodically resets this timer. If the timer ever expires, the bus controller stops sending outputs. If this happens in a Single Bus Genius network of a CPU Redundancy system, the paired GBC in the other unit drives the outputs of the Genius devices. The cause of the failure must be remedied to re-establish communications.

---

## Hardware Configuration for Single Bus Networks

The hardware configuration for single bus networks can be created by selecting *Redundant Controllers, Two PLCs* in the Redundancy Wizard.

The GBCs must be configured with the following settings.

**Redundant Mode:** Redundant Controllers

**Paired GBC:** External

**Serial Bus A:** 31 (primary unit) or 30 (secondary unit)

The redundant devices must be configured for Hot Standby mode. For example, use the following settings for a Genius block:

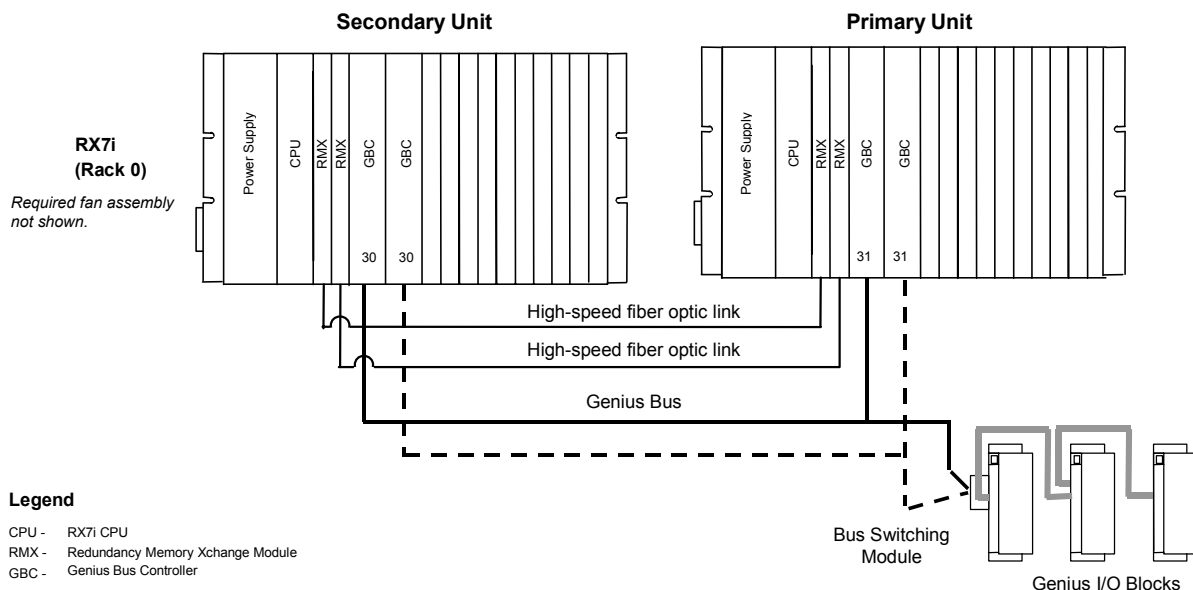
(Programming software) Redundancy = YES

(Hand-Held Monitor) CPU Redundancy = HOT STBY MODE

(Hand-Held Monitor) BSM Present = NO

## Dual Bus Networks

This option provides redundancy of both the PLC and the I/O bus. This type of system uses dual busses with bus controllers in each PLC. A Bus Switching Module (BSM) is required to connect the initial block in the Genius block daisy chain to the dual bus.



The Dual Bus network is suitable if the application requires redundancy of the PLC and the I/O bus.

When using dual bus Genius networks in a Hot Standby CPU Redundancy system, two Bus Controllers for the bus pair must be located in the primary unit and two more in the secondary unit. There can be multiple dual bus pairs. The bus controllers in the primary unit are assigned Serial Bus Address 31. The bus controllers in the secondary unit are assigned Serial Bus Address 30.

Genius output devices will use outputs from Serial bus Address 31 in preference to outputs from Serial bus Address 30. Outputs are determined by the active unit, regardless of which bus controller provides the outputs since all redundant Genius outputs are transferred from the active unit to the backup unit.

Any type of Genius device can be connected to the network. Each Genius network can have up to 30 additional Genius devices connected to it. You may want to reserve one Serial Bus Address for the Hand-Held Monitor.

As a safety feature, a watchdog timer protects each Genius I/O link. The bus controller periodically resets this timer. If the timer ever expires, the bus controller stops sending outputs. If this happens in a Dual Bus Genius network of a CPU Redundancy system, the paired GBC in the other unit drives the outputs of the Genius devices. If the GBC in the other unit is not available, the BSMs switch to the other bus. The cause of the failure must be remedied to re-establish communications.

## Hardware Configuration for Dual Bus Network

The hardware configuration for this type of network can be created by selecting *Dual Bus, Redundant Controllers* in the Redundancy Wizard.

The GBCs must be configured with the following settings

**Redundant Mode:** Dual Bus\_Redundant Controllers

**Paired GBC =** Internal and External

**Serial Bus Address =** 31 (primary unit) or 30 (secondary unit)

The redundant devices must be configured for Hot Standby and dual bus mode. For example, use the following settings for a Genius block:

(Programming Software) Redundancy = YES

(Hand-Held Monitor) CPU Redundancy = HOT STBY MODE\*

(Hand-Held Monitor) BSM Present = YES

(Hand-Held Monitor) BSM Controller = YES (if BSM is mounted) or NO

## Location of GBCs and Blocks

For fastest switching, all Genius Bus Controllers in the Hot Standby CPU Redundancy system should be in the main rack. This will cause the Genius Bus Controller to lose power at the same time that the CPU loses power and allow the backup unit to gain full control of the I/O as soon as possible. Each GBC has an output timer that it resets during every output scan. If the GBC determines that the CPU in its PLC has failed, it will stop sending outputs to its Genius devices. This allows the other GBC to take control of the I/O.

For single and dual bus Genius networks, the Genius bus controllers should be placed at the same end of the bus, as shown on page 2-7. In particular, the secondary unit should be placed at one end of the bus and the primary unit must be placed between the secondary unit and the Genius devices. No I/O blocks or other devices should be located on the bus between the bus controllers.

In the case of dual bus networks, placing the bus controllers and devices in this manner minimizes the risk of a bus break between the two units. A bus break between the units could result in only some devices switching buses, and make the other devices inaccessible to one of the units. It also allows the primary unit to continue to control the I/O in bus failure conditions that might otherwise result in loss of inputs and unsynchronized control of outputs.

Since the recommended configuration for single and dual bus networks still has the possibility of a bus breaking between the two CPUs, you may want to program the application to monitor the status of the busses from the unit configured at the end of the busses and request a role switch or bus switch (dual bus network only) if loss of bus is detected.

## Duplex Genius Output Mode

Although it is not common, you can configure your Genius I/O system for duplex mode, meaning that they will receive outputs from **both** bus controllers 30 and 31 and compare them. Only devices that have discrete outputs can be configured for Duplex mode.

If the controllers at SBAs 30 and 31 agree on an output state, the output goes to that state. If the controllers at SBAs 30 and 31 send different states for an output, the device defaults that output to its pre-selected Duplex Default State. For example:

<i>Commanded State from Device Number 31</i>	<i>Commanded State from Device Number 30</i>	<i>Duplex Default State in the Block or I/O Scanner</i>	<i>Actual Output State</i>
On	On	Don't Care	On
Off	On	Off	Off
Off	Off	Don't Care	Off
On	Off	On	On

If either controller 30 or 31 stops sending outputs to the device, outputs will be directly controlled by the remaining controller.

### ***Local I/O***

Local I/O can be included in either unit; however, ***it is not*** part of the redundant I/O system. A failure in the Local I/O system will affect the unit as described in the *PACSystems CPU Reference Manual*, GFK-2222.

# Chapter 3

## *Configuration Requirements*

---

---

This chapter defines the special configuration requirements of a Hot Standby CPU Redundancy system.

When the program logic will be the same for both units, it is recommended that you use a Dual HWC Target. When you select a Redundancy CPU the programming software automatically presents the Dual HWC Target. A Dual HWC Target is assumed by the remainder of this chapter.

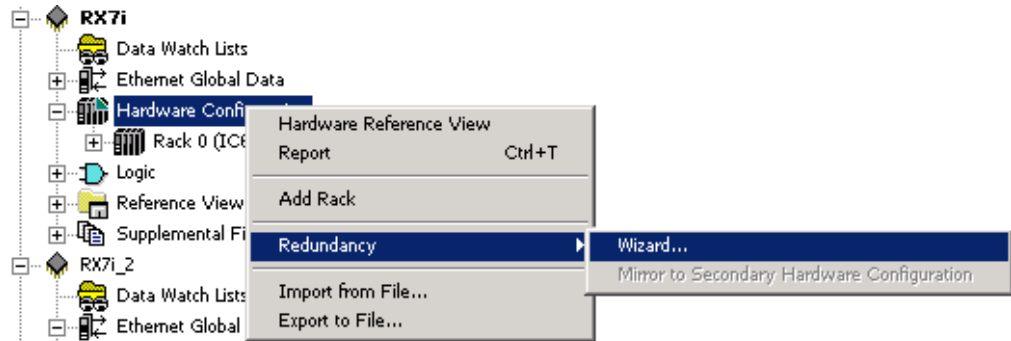
If you do not want to use the same logic in both units, you should create two separate targets and set the target property, Dual HWC to FALSE in each.

### **CAUTION**

**If both units are configured as primary or as secondary, they will not recognize each other. If this happens, the Genius Bus Controllers report SBA conflict faults and flash their LEDs. Correct the configuration of both units before placing either unit in Run mode.**

## Using the Redundancy Wizards

CIMPLICITY Machine Edition software provides redundancy wizards to create a hardware configuration with the correct parameter settings for the redundancy scheme that you choose. See “Configuration Parameters” for details on parameters specific to redundancy systems. To launch the wizard, go to the Navigation window, right click Hardware Configuration, point to Redundancy, and then choose Wizard.



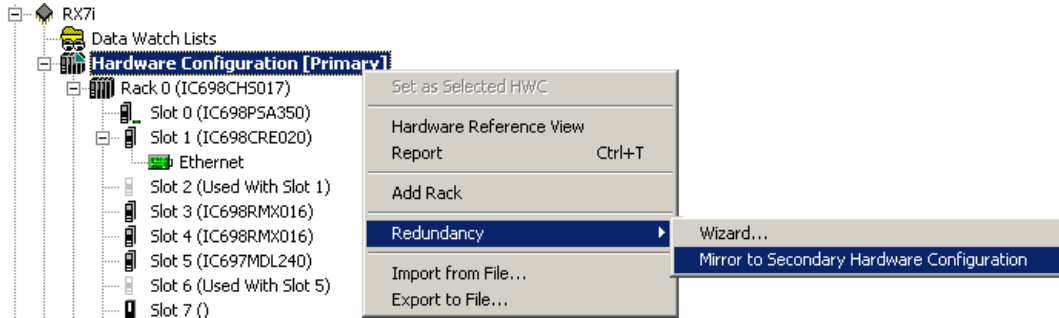
To configure a Hot Standby CPU Redundancy system using the wizards:

1. Run the Set up Primary Hardware Configuration for CPU Redundancy wizard. This wizard configures a redundancy CPU in slot 1 of the main rack and allows you to select the location of the RMX modules used for redundancy links.
2. Run the Add GBCs for Genius Redundancy wizard to configure your Genius bus controllers in the primary unit.
3. Complete configuration of all parameters for the primary unit.
4. When you are finished configuring the primary unit, run the Generate Secondary Hardware Configuration from the Current Configuration wizard. This wizard copies the Primary hardware configuration to the secondary configuration and adjusts appropriate parameters for the secondary configuration.
5. Edit the configuration parameters for each item in the secondary unit's hardware configuration that is unique for the secondary unit (for example, the secondary unit's direct IP address and the CPU's SNP ID).

## Synchronizing the Hardware Configurations

To synchronize the two configurations (after making changes to the Primary configuration or uploading a different primary configuration), right click Hardware Configuration, choose Redundancy, and Mirror to Secondary Hardware Configuration. This command copies the Primary hardware configuration to the secondary configuration and adjusts appropriate parameters for the secondary configuration.

**Note:** You can control whether the contents of specific slots in the Primary configuration are copied to the Secondary configuration. If the Mirror to Secondary property for a slot is set to True (default), the configured module in that slot in the Primary configuration overwrites the corresponding slot in the Secondary configuration. To prevent a slot from being mirrored, set this property to False.



## Configuration Parameters

### CPU Parameters

This section discusses only the parameters that apply to redundancy systems. For information on all the CPU parameters, see the *PACSystems CPU Reference Manual*, GFK-2222.

#### Settings

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>Stop-Mode I/O Scanning</b>	Disabled	N/A	Always Disabled for a Redundancy CPU.
<b>Watchdog Timer (ms)</b>	200	10 through 1000, in increments of 10ms Requires a value that is greater than the program sweep time.	The watchdog timer is designed to detect "failure to complete sweep" conditions. The CPU restarts the watchdog timer at the beginning of each sweep. The watchdog timer accumulates time during the sweep. The watchdog timer is useful in detecting abnormal operation of the application program, which could prevent the PLC sweep from completing within a specified time period. <b>Note:</b> In a CPU redundancy system, the watchdog timer should be set to allow for the maximum expected scan time plus two fail wait times. (The Fail Wait parameter is set on the Redundancy tab.) Furthermore, the watchdog timer setting must allow enough time for the CPU to complete one input data transfer and two output data transfers.

## Scan Parameters

### Communications Window Considerations

The redundancy CPU supports the use of high-speed communications modules such as the Ethernet Interface. Requests from devices attached to these communications modules are handled in the Controller and Backplane Communications windows. Because these requests can be sent in large volumes, there is the potential for either of these windows to be processing requests for a significant amount of time.

One way to reduce the risk of one CPU failing to rendezvous at a synchronization point with the other CPU is to configure the Controller and Backplane Communications windows for Limited Window mode. This sets a maximum time for these windows to run.

Other options are to configure the CPU sweep mode as Constant Window or Constant Sweep. The CPU will then cycle through the communications and background windows for approximately the same amount of time in both units.

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>Sweep Mode</b>	Normal	Normal Constant Window Constant Sweep.	For details on sweep modes, refer to <i>the PACSystems CPU Reference Manual, GFK-2222</i> .
<b>Controller Communications Window Mode</b>	Limited	<b>Limited:</b> Time sliced. The maximum execution time for the Controller Communications Window per scan is specified in the Controller Communications Window Timer parameter. <b>Complete:</b> The window runs to completion. There is no time limit.	(Available only when Sweep Mode is set to <i>Normal</i> .) Execution settings for the Controller Communications Window.
<b>Controller Communications Window Timer</b>	Controller Communications Window Mode is: <b>Limited:</b> 10 <b>Complete:</b> There is no time limit.	Controller Communications Window Mode is: <b>Limited:</b> 0 through 255 ms. <b>Complete:</b> Read only. There is no time limit.	The maximum execution time for the Controller Communications Window per scan.
<b>Backplane Communications Window Mode</b>	Limited	<b>Limited:</b> Time sliced. The maximum execution time for the Backplane Communications Window per scan is specified in the Backplane Communications Window Timer parameter. <b>Complete:</b> The window runs to completion. There is no time limit.	(Available only when Sweep Mode is set to <i>Normal</i> .) Execution settings for the Backplane Communications Window.
<b>Backplane Communications Window Timer (ms)</b>	10ms for Limited mode	<b>Limited:</b> Valid range: 0 through 255 ms. <b>Complete:</b> Read only. There is no time limit.	(Available only when Sweep Mode is set to <i>Normal</i> .) The maximum execution time for the Backplane Communications Window per scan. This value can be greater than the value for the watchdog timer.

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>Background Window Timer</b>	5ms	0 through 255ms	Setting the background window time to zero disables the background RAM tests.
<b>Sweep Timer (ms)</b>	100ms	5 through 2550ms, in increments of 5. If the value typed is not a multiple of 5ms, it is rounded to the next highest valid value.	(Available only when Sweep Mode is set to <i>Constant Sweep</i> .) The maximum overall PLC scan time. This value cannot be greater than the value for the watchdog timer.  Some or all of the windows at the end of the sweep might not be executed. The windows terminate when the overall PLC sweep time has reached the value specified for the Sweep Timer parameter.
<b>Window Timer (ms)</b>	10	3 through 255, in increments of 1.	(Available only when Sweep Mode is set to <i>Constant Window</i> .) The maximum combined execution time per scan for the Controller Communications Window, Backplane Communications Window, and Background Communications Window. This value cannot be greater than the value for the watchdog timer.
<b>Number of Last Scans</b>	0	0-5 (Should be set to 0.)	The number of scans to execute after the PACSystems CPU receives an indication that a transition from Run to Stop mode should occur.  <b>Note:</b> In a redundancy system, this parameter should be set to 0 (default). Using a non-zero value would allow a unit to stay in RUN mode for a few sweeps after detecting a fatal fault.

### Fault Parameters

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
Recoverable Local Memory Error	Diagnostic	Diagnostic Fatal	<b>Redundancy CPUs only.</b> Determines whether a single-bit ECC error causes the CPU to stop or allows it to continue running.

## Redundancy Parameters

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>Redundancy Mode</b>	Primary.	Primary Secondary (Read-only when the Dual HWC target property is set to True.)	Specifies whether the current Hardware Configuration is Primary or Secondary. <b>Note:</b> When the Dual HWC target property is set to True, one Hardware Configuration is automatically set to Primary, and the other, to Secondary.
<b>Control Strategy</b>	HSB	HSB	Selects the HSB control strategy.
<b>Fail Wait Time</b>	60	60 through 400 ms, in increments of 10.	The maximum amount of time this CPU waits for the other CPU to reach a synchronization point. For recommendations on setting Fail Wait time, see chapter 4.
<b>Redundant Links</b>	Determined by number of redundancy links configured for this unit.	Read-only <b>0:</b> The CPU behaves as a redundancy CPU without a backup. <b>1:</b> The CPU behaves as a redundancy CPU with one redundancy link. <b>2:</b> The CPU behaves as a redundancy CPU with two redundancy links. – <b>Strongly Recommended</b>	The number of redundancy links configured for this unit. Each redundancy link is a pair of RMX modules (one in each unit) that have the Redundant Link parameter set to Enabled.
<b>--- Redundant Link 1 ---</b>			
<b>Rack Number</b>	0	(Read only) 0	The rack location of the first RMX module. (Shown only if the Redundant Links parameter is 1 or 2.)
<b>Slot Number</b>	Determined by slot location of RMX module.	(Read-only)	The slot location of the first RMX module. (Shown only if the Redundant Links parameter is 1 or 2.)
<b>--- Redundant Link 2 ---</b>			
<b>Rack Number</b>	0	(Read-only) 0	The rack location of the second redundancy link. (Shown only if the Redundant Links parameter is 2.)
<b>Slot Number</b>	Determined by slot location of RMX module.	(Read-only)	The slot location of the second redundancy link. (Shown only if the Redundant Links parameter is 2.)

## Transfer List

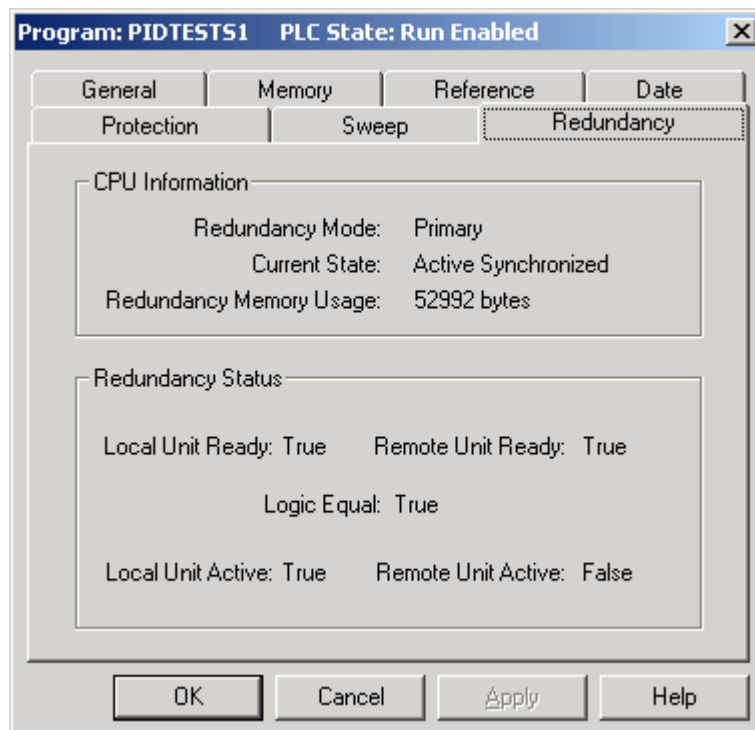
This is where you select which references will be transferred from the active unit to the backup unit. If the program logic requires identical input values for the two units, those references (including Genius inputs) must be included in the input transfer list.

You must include all redundant Genius outputs, i.e. those %Q and %AQ references tied to redundant Genius devices, in the output transfer list. Failure to do so will result in the primary unit always determining the output values, even when it is the backup unit. By default, CIMPLICITY Machine Edition generates an error and prevents store of the configuration if an output is not included in the transfer list. For special situations, you can adjust the Target property, Genius Output, to generate a warning instead.

A maximum of 2Mbytes of data can be included in the transfer list. The amount of data transferred is also limited by the amount of user memory consumption. Overrides and Legacy-style Transitions are also transferred for any specified discrete transfer data, as well as any point fault information for transferred discrete and analog data if Point Faults are enabled. Transferred data, along with user program, configuration, and reference memory size, etc. all count against the user memory size. The amount of data transferred adds to the CPU scan time.

The transfer list configuration must be compatible between the two units.

**Note:** To view the amount of memory used for transfer data (Redundancy Memory Usage), go online and store the configuration. Then right click the Target, choose Online Commands, and select Show Status. In the status dialog box, select the Redundancy tab.



<b>Parameter</b>	<b>Default</b>	<b>Choices</b>	<b>Description</b>
<b>--- Input Memory ---</b>			
<b>%I Reference</b>	%I00001	Must be byte-aligned, that is, it must have a value of $8n + 1$ . Example: %I00025, where $25 = (8 * 3) + 1$ .	The starting address for the range of %I references that are synchronized between the redundant CPUs.
<b>%I Length</b>	0	0 through $(32,768 - Iref + 1)$ , in increments of 8, where Iref = the value set in the %I Reference parameter.	The number of %I references that are synchronized between the redundant CPUs.
<b>%AI Reference</b>	%AI00001	The limit configured for %AI references is based on values provided in the Memory tab. The value of the beginning references plus the value of the length must be less than, or equal to, the configured limit.	The starting address for the range of %AI references that are synchronized between the redundant CPUs.
<b>%AI Length</b>	0	0 through $(AIul - Aref + 1)$ , where AIul = the upper limit of %AI memory configured on the Memory tab, and Aref = the value set in the %AI Reference parameter.	The number of %AI references that are synchronized between the redundant CPUs.
<b>--- Output Memory ---</b>			
<b>%Q Reference</b>	%Q00001	This address must be byte-aligned, that is, it must have a value of $8n + 1$ . Example: %Q00049, where $49 = (8 * 6) + 1$ .	The starting address for the range of %Q references that are synchronized between the redundant CPUs.
<b>%Q Length</b>	0	0 through $(32,768 - Qref + 1)$ , in increments of 8, where Qref = the value set in the %Q Reference parameter.	The number of %Q references that are synchronized between the redundant CPUs.
<b>%M Reference</b>	%M00001	This address must be byte-aligned, that is, it must have a value of $8n + 1$ . Example: %M00121, where $121 = (8 * 15) + 1$ .	The starting address for the range of %M references that are synchronized between the redundant CPUs.
<b>%M Length</b>	0	0 through $(32,768 - Mref + 1)$ , in increments of 8, where Mref = the value set in the %M Reference parameter.	The number of %M references that are synchronized between the redundant CPUs.
<b>%G Reference</b>	%G00001	This address must be byte-aligned, that is, it must have a value of $8n + 1$ . Example: %G00081, where $81 = (8 * 10) + 1$ .	The starting address for the range of %G references that are synchronized between the redundant CPUs.
<b>%G Length</b>	0	0 through $(7,680 - Gref + 1)$ , in increments of 8, where Gref = the value set in the %G Reference parameter.	The number of %G references that are synchronized between the redundant CPUs.
<b>%AQ Reference</b>	%AQ00001	The limit configured for %AQ references is based on values provided in the Memory tab. The value of the beginning reference address plus the value of the length must be less than, or equal to, the configured limit.	The starting address for the range of %AQ references that are synchronized between the redundant CPUs.

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>%AQ Length</b>	0	0 through (AQul - AQref + 1), where AQul = the upper limit of %AQ memory configured on the Memory tab, and AQref = the value set in the %AQ Reference parameter.	The number of %AQ reference addresses that are synchronized between the redundant CPUs. The limit configured for %AQ references is based on values provided in the Memory tab. The value of the beginning reference plus the value of the length must be less than, or equal to, the configured limit.
<b>%R Reference</b>	%R00001	The limit configured for %R references is based on values provided in the Memory tab. The value of the beginning references plus the value of the length must be less than, or equal to, the configured limit.	The starting address for the range of %R references that are synchronized between the redundant CPUs.
<b>%R Length</b>	0	: 0 through (Rul - Rref + 1), where Rul = the upper limit of %R memory configured on the Memory tab, and Rref = the value set in the %R Reference parameter.	The number of %R reference addresses that are synchronized between the redundant CPUs. The limit configured for %R references is based on values provided in the Memory tab. The value of the beginning address plus the value of the length must be less than, or equal to, the configured limit.
<b>%W Reference</b>	%W00001	The limit configured for %W references is based on values provided in the Memory tab. The value of the beginning reference address plus the value of the length must be less than, or equal to, the configured limit.	The starting address for the range of %W references that are synchronized between the redundant CPUs.
<b>%W Length</b>	0	0 through (Wul - Wref + 1), where Wul = the upper limit of %W memory configured on the Memory tab, and Wref = the value set in the %W Reference parameter.	The number of %W references that are synchronized between the redundant CPUs. The limit configured for %W references is based on values provided in the Memory tab. The value of the beginning reference address plus the value of the length must be less than, or equal to, the configured limit.

**Redundancy Memory Xchange Modules**

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>Redundant Link</b>	Enabled	Enabled Disabled	If the RMX module is being used as a redundancy link, this parameter must be set to Enabled. An RMX module being used as a redundancy link cannot be used as a general-purpose reflective memory module. All the reflective memory parameters are unavailable, and the Interrupt parameter is set to Disabled.

## Ethernet Interface

Each unit contains at least one Ethernet interface that is assigned a direct IP address used to directly access the specific unit. A third, redundant, IP address can be assigned to the pair of Ethernet interfaces in both the primary and secondary units. The redundant IP address is active on the Ethernet interface in only one of the units at a time, the active unit. All data sent to the redundant IP address (including EGD produced to the redundant IP address) is handled by the active unit. When active, the Ethernet interface always initiates communications using the redundant IP address. When the unit is not active, all communications are initiated through the direct IP address. For more information about the Redundant IP address, refer to “Redundant IP Addresses” in chapter 4.

You can have up to four Ethernet interfaces in each rack, including the CPU’s embedded Ethernet interface. Each Ethernet interface can be set up as part of a pair for the purposes of redundant IP. (You can also include Ethernet interfaces in the unit that are not part of a redundant IP pair.)

When an Ethernet Interface is configured to produce Ethernet Global Data (EGD), you must configure a redundant IP address in addition to the direct IP address. For more information about using EGD in a redundant system, see chapter 4.

<i>Parameter</i>	<i>Default</i>	<i>Choices</i>	<i>Description</i>
<b>IP Address</b>	0.0.0.0	x.x.x.x where x ranges from 1 to 255	This IP address, also known as the <i>direct IP address</i> , always applies only to this unit.  The IP Address should be assigned by the person responsible for your network. TCP/IP network administrators are familiar with these sorts of parameters and can assign values that work with your existing network. If the IP address is improperly set, your device may not be able to communicate on the network and could disrupt network communications.
<b>Redundant IP</b>	Disable	Disable Enable	(Available only when the target’s CPU is a redundancy CPU.) Enabling this feature allows the Ethernet Interface to share an IP address with the corresponding Ethernet Interface in the other unit.
<b>Redundant IP Address</b>	0.0.0.0	x.x.x.x where x ranges from 1 to 255	(Available only when the Redundant IP parameter is set to Enable.) The IP address shared by two Ethernet Interfaces that are connected to the same network and reside in separate units (one in the primary unit and the other in the secondary unit). Although the redundant IP address is shared by both Ethernet Interfaces, only the Interface in the active unit responds to this IP address.  For a given pair of Ethernet Interfaces, the redundant IP address must be the same value on the primary and secondary units.  The redundant IP address should be assigned by the person responsible for your network. TCP/IP network administrators are familiar with these sorts of parameters and can assign values that work with your existing network. If the IP address is improperly set, your device may not be able to communicate on the network and could disrupt network communications.  <b>Note:</b> The redundant IP address must not be the same as the direct IP address of either Ethernet Interface. The redundant IP address must be on the same sub-network as the direct IP address.

## Rack Module Configuration Parameters

- Interrupts cannot be ENABLED when the configured CPU is a Redundancy CPU. When a redundant CPU is configured, any interrupts enabled in the configuration are set to DISABLED.

## Bus Controller Configuration Parameters

- When configuring the PRIMARY PLC, all Genius Bus Controllers configured for external redundancy must have Serial Bus Address 31.
  - When configuring the SECONDARY PLC, all Genius Bus Controllers configured for external redundancy must have Serial Bus Address 30.
- Note:** It is possible to configure Genius networks in which there is not a redundant bus controller in the other unit. It is not necessary for the serial bus addresses to be 31 in the primary unit and 30 in the secondary unit for such networks.
- For single Genius bus networks, the Genius Bus Controllers must be configured for RED CTRL Redundancy with the redundant pair set to EXTERNAL.
  - For Dual Bus Genius networks, the Genius Bus Controllers must be configured for Dual Bus/Redundant Controller.
- Note:** Genius Bus Controllers for networks that are connected to just one unit may have any setting.

## Genius Device Configuration Parameters

All of the Genius devices that are connected to both units must be configured as redundant.

**Note:** Devices that are connected to just one unit may use any available setting.

## Storing (Downloading) Hardware Configuration

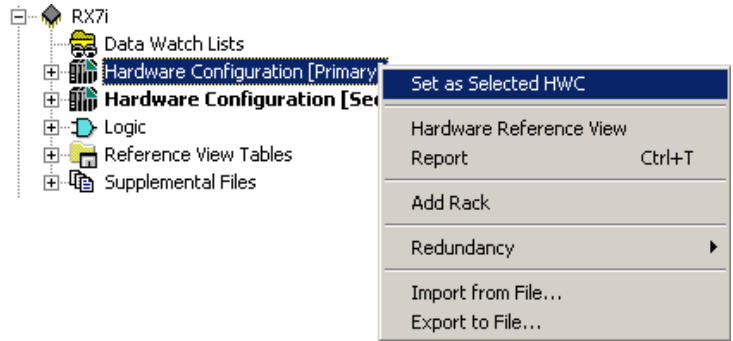
A PACSystems control system is configured by creating a configuration file in the programming software, then transferring (downloading) the file from the programmer to the CPU via the Ethernet Interface or serial port. You can communicate with the CPU using either the embedded or the rack based Ethernet interface or the serial port. The CPU stores the configuration file in its non-volatile RAM memory.

In the programming software all online operations, including downloading a folder, are performed on the PLC that is the selected hardware configuration. You must download the hardware configuration to each PLC in the redundancy system in a separate operation.

### CAUTION

**If both units are configured as primary or as secondary, they will not recognize each other. If this happens, the Genius Bus Controllers report SBA conflict faults and flash their LEDs. Correct the configuration of both units before placing either unit in Run mode.**

1. Make sure the primary HWC is selected.  
To select a hardware configuration, right click on Hardware Configuration and choose Set as Selected HWC.



2. If not already done, set the physical port parameters for the primary unit in the Target properties.
3. Connect to the CPU. Make sure the CPU is in Stop mode.
4. Download.
5. Go offline.
6. Select the secondary HWC.
7. If not already done, set the physical port parameters for the secondary unit in the Target properties.
8. Connect to the CPU. Make sure the CPU is in Stop mode.
9. Download.

## Configuring the Redundancy CPU for Non-redundant Operation

The Redundancy CPU can be used for both redundant and non-redundant applications. For non-redundant applications do not configure any redundancy links.

# Chapter 4

## Operation

---

---

This chapter discusses aspects of PACSystems CPU operation that function differently in a redundancy system. For general details of CPU operation, refer to the PACSystems CPU Reference Manual, GFK-2222.

- Powerup of a Redundant CPU
- Synchronizing Redundant CPUs
- HSB Control Strategy
- %S References for CPU Redundancy
- Scan Synchronization
- Fail Wait Time
- Data Transfer
- Switching Control to the Backup Unit
- RUN Disabled Mode
- Error Checking and Correction
- Timer and PID Functions
- Timed Contacts
- Multiple I/O Scan Sets
- Stop to Run Mode Transition
- Genius Bus Controller Switching
- Redundant IP Addresses

## *Powerup of a Redundancy CPU*

When a redundant CPU is powered up, it performs a complete hardware diagnostic check and a complete check of the application program and configuration parameters. This causes the powerup time of a redundancy CPU to be longer than a non-redundancy CPU. If the primary and secondary units power up together, the primary becomes the active unit and the secondary unit becomes the backup unit.

When the secondary unit powers up, if it does not detect the primary unit, the secondary unit waits up to 30 seconds for the primary unit to power up. If the primary unit has not completed its powerup sequence within 30 seconds, the secondary unit assumes the primary unit is not present. In this case, if the secondary unit is setup to transition to Run on powerup, it becomes an active unit without a backup unit.

If the primary unit completes its powerup sequence before the secondary unit, the primary unit waits a few seconds for the secondary unit to complete its powerup sequence. If the primary unit is set up to transition to Run on powerup and does not detect the secondary unit within this time, it becomes an active unit without a backup.

**Note:** If the system should be fully redundant upon powerup, the secondary unit must complete power-up first but no more than 30 seconds before the primary unit. The way to be sure this happens is to apply power to the secondary unit first.

If either unit is powered up after the other unit is already in Run mode, communications between the two units are established. If the unit being powered up goes to Run mode, a resynchronization occurs.

## *Synchronization of the Time of Day Clocks*

At the point when the two units establish communications, the primary unit's time of day clock is copied to the secondary unit.

## *Synchronizing Redundant CPUs*

When synchronization is initiated, the CPUs exchange information about their configurations. If a transitioning CPU detects that the configurations are not in agreement, that CPU will not transition to RUN mode; if both CPUs are transitioning at the same time, neither CPU transitions to RUN mode. The following items must be in agreement in order to synchronize:

1. Both CPUs must be configured for the same redundancy control strategy.
2. Both CPUs must have compatible transfer lists.
3. If %I, %Q, %AI, or %AQ references are included in the transfer list, the Point Fault References configuration parameter must be identical on both units.

### **Dual Synchronization**

Dual Synchronization occurs when both CPUs transition to Run at the same time. The primary unit becomes the active unit and the secondary unit becomes the backup unit. Non-retentive data is cleared, and the #FST\_SCN reference and #FST\_EXE bits are set to 1.

### **Resynchronization**

Resynchronization occurs when one unit is already in Run mode and the other unit is put into Run mode. The transitioning unit attempts to get back in synchronization with the currently active unit. The transitioning unit becomes the backup unit.

At this point, the active unit sends the output transfer data and the input transfer data to the backup unit. In addition to the configured redundancy transfer data, the #FST\_SCN %S reference as well as internal timer information and #FST\_EXE for each common logic block are transferred from the active unit to the backup unit. Only the internal timers and #FST\_EXE data for program blocks with the same name are transferred. Therefore, the #FST\_SCN and #FST\_EXE bits for common blocks are not set on the first scan of the transitioning unit.

## *HSB Control Strategy*

In the HSB control strategy, Genius outputs are always enabled for both units (unless explicitly disabled) so that bumpless switching is possible regardless of which unit is currently the active unit. The user is required to include all redundant Genius outputs in the output transfer list so that both units.

If both units power up together and go to RUN mode, the primary unit becomes the active unit and the secondary unit becomes the backup unit.

If one of the units is already in RUN mode and the other unit goes to RUN mode, the unit already in RUN mode remains the active unit and the transitioning unit becomes the backup unit. The behavior is the same whether the unit going to RUN is the primary unit or the secondary unit.

## *%S References for CPU Redundancy*

%S33 through %S39 and %SB18 reflect the status of the redundancy units. The table below describes these %S references, and shows their expected states, assuming the primary unit is active and the secondary unit is backup.

%S Bit	Definition	Name	Description	Expected State	
				Primary Unit	Secondary Unit
%S33	Primary Unit	#PRI_UNT	Set to 1 if the local unit is configured as the primary unit; otherwise, it is cleared. For any given local unit, if PRI_UNT is set, SEC_UNT cannot be set.	ON	OFF
%S34	Secondary Unit	#SEC_UNT	Set to 1 if the local unit is configured as the secondary unit; otherwise, it is cleared. For any given local unit, if SEC_UNT is set, PRI_UNT cannot be set.	OFF	ON
%S35	Local Unit Ready	#LOC_RDY	Set to 1 if local unit is in Run mode with outputs enabled. Other wise set to 0.	ON	ON
%S36	Local Unit Active	#LOC_ACT	Set to 1 if local unit is currently the active unit; otherwise it is cleared. For any given local unit, if LOC_ACT is set, REM_ACT cannot be set.	ON	OFF
%S37	Remote Unit Ready	#REM_RDY	Set to 1 if remote unit is in Run mode with outputs enabled. Otherwise set to 0.	ON	ON
%S38	Remote Unit Active	#REM_ACT	Set to 1 if remote unit is currently the active unit; otherwise it is cleared. For any given local unit, if REM_ACT is set, LOC_ACT cannot be set.	OFF	ON
%S39	Logic Equal	#LOGICEQ	Set to 1 if the application logic for both units in the redundant system is the same. Otherwise set to 0.	ON	ON
%SB18	Redundancy Informational Message Logged	#RDN_MSG	Set if a redundancy informational message was logged. It can be cleared in reference tables, logic, or by clearing the fault tables.		

%S references can be read from the application program, but cannot be altered or overridden. These references are always OFF when no configuration has been stored. Anytime a configuration is stored, the states of these %S references are updated in both STOP and RUN modes.

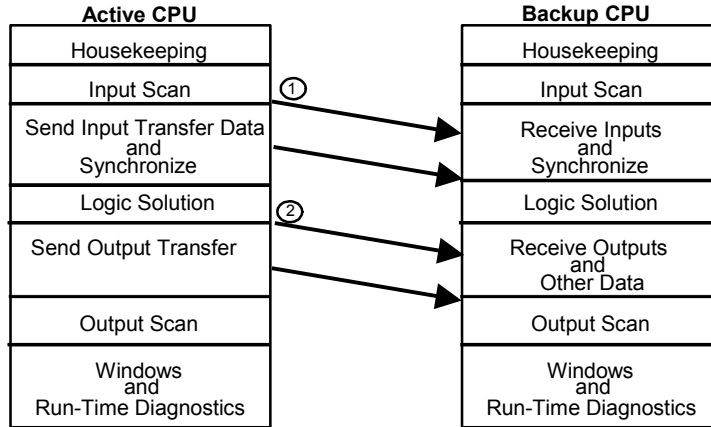
The four redundancy status LEDs on the RMX Module correspond to the %S35, %S36, %S37, and %S38 references. The programming software summarizes the state of the redundancy system on the Redundancy tab of the Show Status dialog box, accessed from Online commands. Additionally, external indicators can be used to monitor the state of any status reference.

### **#OVR\_PRE %S Reference Not Available**

The #OVR\_PRE reference, %S00011, which indicates whether one or more overrides is active, *is not* supported by the Redundancy CPU and should not be used.

## Scan Synchronization

The figure below shows the sweep components for the active and the backup CPUs.



- ① Input data transfer: %I, %AI
- ② Output data transfer: %Q, %AQ, %R, %M, %G, %W

There are two synchronization points in the sweep. The first synchronization point occurs immediately after the inputs are scanned. At this point in the sweep, the newly-read inputs are sent from the active unit to the backup unit. In the second synchronization point, the rest of the data (outputs, internal references, registers) is sent from the active unit to the backup unit. These data transfers are automatic; they require no application program logic (but **do** require proper configuration).

Data can be transferred on either redundancy link. If one link fails, the transfer switches to the other link without causing a loss of synchronization.

---

## *Fail Wait Time*

The active and backup CPUs synchronize their execution twice each sweep: once before logic execution and once afterwards. Certain failures of one CPU, such as an infinite loop in the logic, are detected by the other CPU as a failure to reach the next synchronization point on time. The maximum time to wait for the other CPU is known as the *Fail Wait* time. The duration of this time must be specified during configuration of both the Primary and Secondary Units and can range from 60 ms to 400 ms (in increments of 10 ms), with the default being 60 ms.

The configured Fail Wait time for the system must be based on the maximum expected or allowable difference in the two CPUs reaching a synchronization point. For example, if one CPU might spend 20ms the communications phase of the sweep and the other unit might spend 95ms in communications in the same sweep, the Fail Wait time must be set to at least 80ms ( $80 > 95 - 20$ ) to prevent accidental loss of synchronization. Differences in the logic execution time and other phases must also be considered when selecting a Fail Wait time. Some applications limit the possible difference during the communications window by using Constant Sweep mode or Constant Window mode, or by setting the system communications window to LIMITED and selecting a small window time.

## Data Transfer

The data is transferred in blocks. Each block is checked for data integrity. The backup CPU holds the transferred data in a temporary area until all the data has been received and verified. Then the backup CPU copies the data into the actual PLC memories. If the full transfer fails to complete properly, the backup unit becomes an unsynchronized active unit and discards the data in the temporary area.

## Input Data and Synchronization Data Transfer to the Backup Unit

Immediately after the Input Scan, the active unit sends the selected input data (%I, %AI) to the backup unit. For discrete data, the status, override, and legacy-style transition information is transferred. If point faults are configured, point fault data is also sent.

## Sweep Time Synchronization

During the first transfer, the active unit automatically sends a synchronizing message to the backup unit. This message contains the Start of Sweep Time. The CPUs stay synchronized because the active unit waits for the backup CPU to respond to the synchronizing message before starting its logic execution.

The Start of Sweep Time message transfer repeatedly coordinates the elapsed time clocks (upon which timers are based) in the redundant CPUs. The system time is continuous as long as one of the two systems is running. When a switchover occurs, the same time continues to be kept in the new active unit.

## Transition Contacts and Coils

PACSystems supports two types of Transition contacts and coils:

- Legacy Transition contacts and coils: POSCON, NEGCON, POSCOIL, and NEGCOIL
- IEC Transition contacts and coils: PTCON, NTCON, PTCOIL, and NTCOIL

The essential difference between the two types of instruction is that each IEC transitional used in logic has its own associated instance data. The instance data gives the state (ON or OFF) of the BOOL variable associated with the contact or coil the last time it was executed. For additional information on Transition contacts and coils, refer to the *PACSystems CPU Reference Manual*, GFK-2222.

For any redundant transfer data item placed in a transfer list that is located in a discrete reference table or in the symbolic discrete reference region, the associated Override and legacy-style Transition data is transferred as part of that list. However, the instance data associated with IEC transitionals is **not** synchronized. For this reason, IEC transitionals should not be used in redundancy.

---

## Output Data Transfer to the Backup Unit

After the input data transfer, both units operate independently until the end of the program logic solution. Before the output scan starts, a second automatic data transfer occurs. At this time, the active unit transfers the output transfer data to the backup unit. This includes the %Q, %AQ, %R, %M, %G, %W memories. For discrete data, the status, override, and legacy transition information is transferred. If point faults are configured, point fault data is also sent.

After the output data transfer, the active and the backup units independently perform their output scans and run their communications and background windows. They continue to operate independently until they synchronize again after the next input scan.

## Data Transfer Time

When a system is synchronized, there are additions to the sweep time (compared to a similar non-redundant CPU model) for transferring data from one unit to the other. The data transfer time includes the time for the active unit to read the data from the appropriate reference memory type as specified in the configured redundancy transfer list, move it from the CPU memory across the backplane, with appropriate data integrity information, into the RMX on-board memory. The data is then transferred from the RMX module in the active unit to the backup unit's RMX module via a high-speed fiber optic link. On the backup unit, the data is moved from the RMX on-board memory over the backplane into the CPU memory. A data integrity check is performed, and assuming the integrity checks pass, the transfer data is written to the appropriate reference memory in the backup unit. These additions to the sweep time can be estimated using the data and equations given in this section.

First, calculate the total number of bytes included in the transfer data.

<b>Reference Type</b>	<b>Reference Size</b>	<b>If Point Faults are Disabled:</b>	<b>If Point Faults are Enabled:</b>
%I	Bit	$(\%I \text{ length} \times 3) \div 8$	$(\%I \text{ length} \times 4) \div 8$
%AI	Word	$(\%AI \text{ length} \times 2)$	$(\%AI \text{ length} \times 3)$
%Q	Bit	$(\%Q \text{ length} \times 3) \div 8$	$(\%Q \text{ length} \times 4) \div 8$
%M	Bit	$(\%M \text{ length} \times 3) \div 8$	
%G	Bit	$(\%G \text{ length} \times 3) \div 8$	
%AQ	Word	$(\%AQ \text{ length} \times 2)$	$(\%AQ \text{ length} \times 3)$
%R	Word	$(\%R \text{ length} \times 2)$	
%W	Word	$(\%W \text{ length} \times 2)$	

Then, use the following formulas to estimate the data transfer time.

### Transfer Time for Redundancy CPU – CRE020

Synchronization base sweep addition – additional amount of time required to synchronize the CPUs with 0 Data Transfer (ms)	3.234 ms
Estimated time for Data Transfers less than 28K bytes (ms)	$(0.00018355 \times (\text{Total Bytes Transferred})) + 0.184$
Estimated time for Data Transfers greater than 28K bytes (ms)	$(0.00013738 \times (\text{Total Bytes Transferred})) + 1.954$

Analysis of the resulting linear curve based on the measurement of various data points, yielded a break point around 28K, resulting in the two linear equations stated above. Using the proper equation for the amount of transfer data will yield a minimum amount of error when doing the calculation. The actual data transfer time may vary slightly from the estimated time; most systems will see slightly better performance than the estimated value. In addition, the estimated data transfer time is based on a redundant system with two redundancy links in a steady state non-error condition without CPU serial communications activity, Genius bus faults or other high backplane interrupt activity.

## Programming a Data Transfer from Backup Unit to Active Unit

The program logic can be used in both CPUs to transfer eight bytes (four registers) of data from the backup unit to the active unit before the next logic solution.

To initiate this transfer, the backup unit executes SVC\_REQ #27 (Write to Reverse Transfer Area). This command copies eight bytes of data from the reference in the backup unit specified by the PARM parameter. Note that SVC\_REQ #27 only works when its CPU is the backup unit. When its CPU is the active unit, SVC\_REQ #27 has no effect.

The active unit stores the transferred data in a temporary buffer. The program in the active unit must execute SVC\_REQ #28 (Read from Reverse Transfer Area), which copies the eight bytes of data from the temporary buffer to the reference specified by the PARM parameter. SVC\_REQ #28 only works in the active unit. It has no effect when its CPU is the backup unit.

There is always a one-sweep delay between sending data from the backup unit using SVC\_REQ #27 and reading the data at the active unit using SVC\_REQ #28.

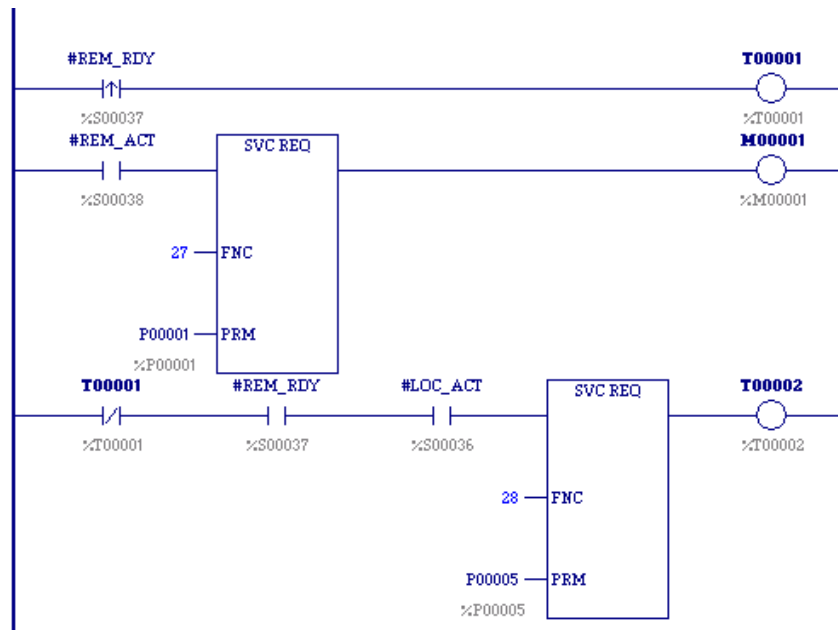
This data copied from the buffer is not valid in the following cases:

- during the first scan after either unit has transitioned to RUN;
- while the backup unit is in STOP mode;
- if the backup unit does not issue SVC\_REQ #27.

The data should not be used if #REM\_RDY is off or if #REM\_RDY is transitioning to on.

### Reverse Data Transfer Example

The following rungs would be placed in the program logic of both units. In this example, the backup unit would send %P0001 through %P0004 to the active unit. The active unit would read the data into %P0005 through %P0008. %P0001 through %P0004 on the active unit and %P0005 through %P0008 on the backup unit would not change. %T0002 would be set to indicate that the operation was successful and that the data could be used.



## Disabling Data Transfer Copy in Backup Unit (SVC\_REQ #43)

Service Request function block #43 instructs the backup unit to bypass the copy of the transfer data from the active unit to the backup unit. It can be used to help determine if the backup unit is collecting inputs properly (that is, validate the input scan). It can also be used to help determine whether the backup unit is calculating outputs and internal variables properly (that is, validate the logic solution).

This function is valid only when issued in the backup CPU. It is ignored if issued when the units are not synchronized, or if it is issued in the active unit.

SVC\_REQ #43 disables the copy of data for 1 sweep beginning with the output data transfer and ending with the input data transfer of the next sweep. The copy can be disabled for multiple sweeps by invoking SVC\_REQ #43 once each sweep for the appropriate number of sweeps.

The resynchronization data transfer always occurs, even if SVC\_REQ #43 is invoked in the first sweep after synchronization (this data transfer includes all inputs, outputs, and internal data that must be exchanged) since the resynchronization data transfer occurs before the start of logic execution.

This function can be set up to disable the copies for all transfers or just the output transfers. If just the output copy is disabled, the two units can still use the same set of inputs on each unit. This makes it possible to test the ability of the two units to derive the same results from the same inputs.

In all cases, the data is still transferred over the redundancy link every sweep and the synchronization points are still met. The effect of SVC\_REQ #43 is to disable the copy of the data from the transfer to the actual reference memories on the backup unit.

### Warning

**When SVC\_REQ #43 is in effect, the backup unit will still take control of the system in event of a failure or role switch. Switches to the backup unit may cause a bump of the outputs since the two units may not be generating the exact same results.**

Consider disabling outputs on the backup unit while SVC\_REQ #43 is in effect. Disabling outputs on the backup unit eliminates the risk of an unsynchronized switch of control (which can cause a bump in the outputs) if the active unit fails or loses power while the input/output copies are disabled. However, if the active unit does fail or loses power while outputs are disabled on the backup unit, the system's outputs will go to their default settings. A secondary effect of disabling outputs on the backup unit is that the non-synchronized fault action table is used by the active unit to determine which faults are fatal.

**Note:** If the CPU is already in RUN/ENABLED mode, a command to disable its outputs will not take effect until one sweep after the command is received. Therefore, disable the outputs at least one sweep before you enable SVC\_REQ #43.

SVC\_REQ #43 cannot be used to disable output data transfer on the primary unit when outputs are enabled on the primary unit. If that is attempted, the function block is rejected.

A fault is logged the first time SVC\_REQ #43 is used as a warning that the PLCs are not completely synchronized.

The reverse data transfer, if any, is unaffected by this function block.

Enabling logic should be used with SVC\_REQ #43. A contact with a non-transferred reference should be part of this enabling logic. That will allow the function block to be turned on/off directly without being overwritten by the value from the active unit.

If the function block is invoked multiple times in a single sweep, the last call is the one that determines the action taken.

### Command Block for SVC\_REQ #43

The command block for the Disable Data Transfer Copy service request function block (SVC\_REQ #43) is as follows:

Format	Address
Disable Copies Selection	Address +2

The first parameter is a word that represents the input parameter format for this Service Request. It must be set to 0.

The second parameter is the word that specifies which data transfers to disable: Input and Output or Output only. The valid values are:

Disable input and output copies	1
Disable output copy only	2

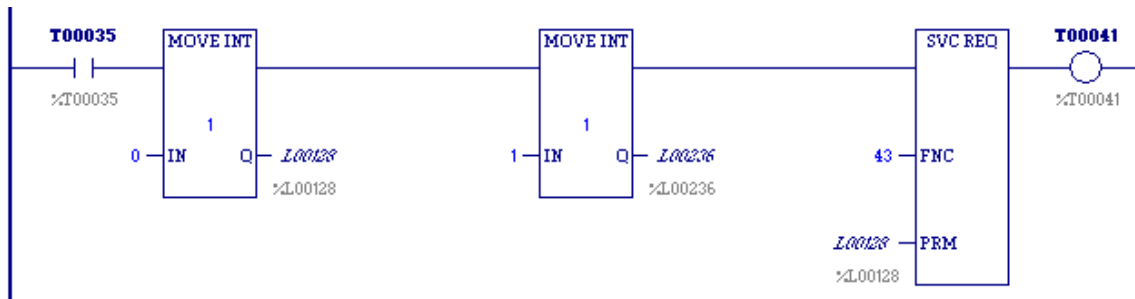
Successful execution occurs unless:

1. The Format parameter is non-zero
2. The Disable Copies Selection parameter is neither 1 nor 2.
3. The function block is invoked when the two units in a redundant system are not synchronized.
4. The function block is issued on the active unit.
5. The function block is issued on the primary unit while the primary unit's outputs are enabled.

Unsuccessful execution will not turn on power flow for the function block.

### Example

In the following example, when %T00035 is on, the input and output copies are disabled.



## Backup Qualification with SVC\_REQ #43

Service Request function block #43 can be used to help determine if the backup unit is collecting inputs properly (that is, validate the input scan). It can also be used to help determine whether the backup unit is calculating outputs and internal variables properly (that is, validate the logic solution). Instructions are given below.

### Validating the Backup PLC's Input Scan

To determine whether the backup PLC is collecting inputs properly, follow these steps:

1. Activate SVC\_REQ #43 on the backup CPU, passing "0, 1" to disable the input and output data transfer copies.
2. Observe the backup unit's %I and %AI reference tables. The values in these tables correspond to the inputs that the backup is currently collecting.
3. Visually compare the backup unit's %I and %AI reference tables with the active unit's tables. Pay special attention to the %I and %AI references that are configured to be transferred between the two units.
4. When you are satisfied that the backup unit is collecting inputs properly, disable the rung that calls SVC\_REQ #43.

### Validating the Backup PLC's Logic Solution

To determine whether the backup unit is calculating outputs and internal variables properly, follow these steps:

1. Activate SVC\_REQ #43 on the backup CPU, passing "0, 2" to disable the output data transfer copy.
2. Observe the backup unit's %Q, %AQ, %M, %G, %R, and %W reference tables. The values in these tables correspond to the values that the backup is currently calculating.
3. Visually compare the backup unit's %Q, %AQ, %M, %G, %R, and %W reference tables with the active unit's tables. Pay special attention to those references that are configured to be transferred between the two units.
4. When you are satisfied that the backup unit is calculating outputs and internal variables properly, disable the rung that calls SVC\_REQ #43.

## ***Switching Control to the Backup Unit***

Control switches from the active unit to the backup unit if:

1. The active unit detects a fatal fault.
2. The active unit is placed in Stop mode.
3. The active unit fails or is powered off.
4. The toggle switch on an RMX module is activated.\*
5. A switch is commanded from the application program.\*

\*These two types of requests are not honored if they occur within 10 seconds of the previous request.

## **Switching Times**

The amount of time needed to switch control from the active unit to the backup unit depends on the reason for the switch.

There are two ways that the backup unit detects that the active unit has failed or lost power:

- A. Failure of all remaining redundancy links.
- B. Failure of the active unit to rendezvous at a synchronization point within the Fail Wait time.

For these two cases the switchover occurs immediately.

For all other cases, the switchover occurs just before the next input data transfer. The maximum delay is 1 sweep. There may be an input and an output scan between detection of the fatal fault and the switch.

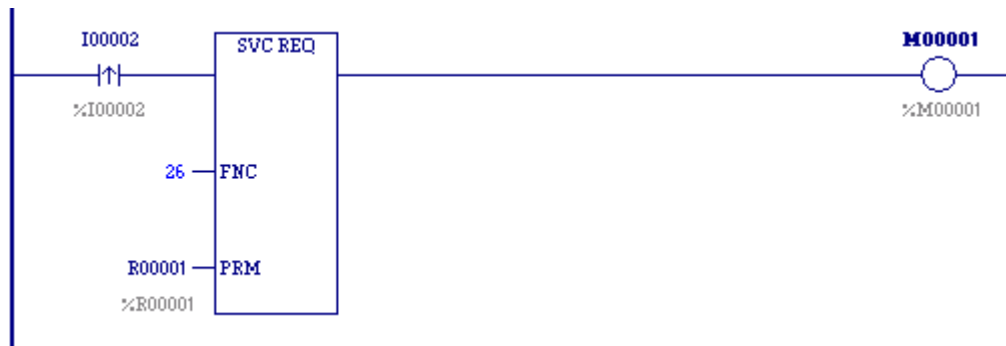
## **Commanding a Role Switch from the Application Program (SVC\_REQ #26)**

The application program can use SVC\_REQ #26 to command a role switch between the redundant CPUs (active to backup *and* backup to active). As long as the units remain synchronized, the switch occurs just before the input data transfer of the next sweep.

When SVC\_REQ #26 receives power flow to its enable input, the PLC is requested to perform a role switch. Power flow from SVC\_REQ #26 indicates that a role switch will be attempted on the next sweep. Power flow *does not* indicate that a role switch has occurred or that a role switch will definitely occur on the next sweep. The role switch request is not valid if it occurs within 10 seconds of a previous request. The 10-second limitation guarantees that only a single switch occurs if a request is made by both units at approximately the same time. The PARM parameter is ignored by SVC\_REQ #26; however the programming software requires that an entry be made for PARM. You can enter any appropriate reference here; it will not be used.

**Example**

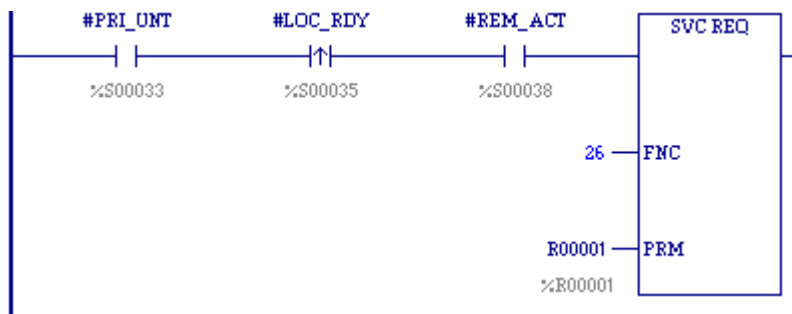
In this example, a pushbutton switch on a control console is wired to input %I0002. In the program logic, the reference for %I0002 is used as the input to the SVC\_REQ #26 function block. When the button is pressed, logic power flows to SVC\_REQ #26, causing a role switch to be requested.



**Implementing Preferred Master Using SVC\_REQ #26**

The HSB control strategy implements a floating master algorithm. This means that when one unit is put into Run mode while the other unit is already in Run mode, the transitioning unit always becomes the backup unit.

If an application requires a preferred master algorithm where the primary unit always becomes the active unit when placed in Run mode, the logic can use the Role Switch service request, SVC\_REQ 26, as shown in the sample LD rung below. This logic must be included in the primary unit and may also be included in the secondary unit.



## ***RUN Disabled Mode***

RUN/DISABLED mode causes all physical outputs to go to their default state in that PLC. Inputs are still scanned and logic is solved. A CPU in RUN/DISABLED mode *may be* the active unit.

The following guidelines apply to using RUN/DISABLED mode with the HSB control strategy.

1. If a unit is in RUN/DISABLED mode, its #LOC\_RDY %S reference and the other unit's REM\_RDY %S reference are not set and the corresponding LEDs on the RMX modules are OFF. This indicates that the unit (with #LOC\_RDY reference off) is not available to drive outputs.
2. If a unit is in RUN/ENABLED mode and the other unit is in RUN/DISABLED mode, the unit in RUN/ENABLED mode does not use its synchronized fault action table. Instead, it uses the user-configurable fault actions since there is no backup available to drive outputs.
3. Since redundant Genius outputs are always transferred from the active unit to the backup unit, if outputs are enabled on either unit, the redundant Genius devices receive the output values calculated by the active unit.

**Note:** If the backup unit is in RUN/DISABLED mode, the backup unit continues NOT to drive outputs upon failure of the active unit and *therefore is not a complete backup*.

## ***Error Checking and Correction***

ECC allows the CPU firmware to detect certain parity bit errors in memory and correct some of them on the fly. This added layer of checking differs from parity checking in that it can correct the bit error. If ECC detects an error that it cannot correct, it generates a system fault. If the ECC error is a single-bit corrected error, the CPU generates a diagnostic fault and sets %SA0006 so that you can know of a possible impending problem and take corrective action. If the ECC error is a multi-bit error, which cannot be corrected, the CPU logs a fatal fault and goes to Stop-Halt mode.

## Timer and PID Functions

Timer and PID function blocks remain in lock step between two synchronized units provided:

- A. Enabling logic for each function is identical on both units. This includes power flow, how often the block is called, and so forth.
- B. The block in which the function occurs has the same name in both units. Note that `_MAIN` is always common.
- C. Reference registers (3 for timers, 40 for PID), enabling references, and reset references for each timer and PID function block are included in the data transfer lists.

For example, if the following ladder logic appears in the `_MAIN` block on both units, `%M100`, `%R250`, `%R251`, and `%R252` must all be included in the output data transfer list to keep this timer synchronized between the two units:



## Timed Contacts

When both systems are synchronized, timed contacts (`%S3`, `%S4`, `%S5`, `%S6`) have exactly the same value in both units. For example, whenever `T_SEC` is on in one unit, it also is on in the other unit as long as both units are synchronized.

## Multiple I/O Scan Sets

The Redundancy CPU supports the configuration of multiple scan sets. However, it is strongly recommended that the redundant I/O be configured in the default scan set (Scan set 1), which is scanned every sweep. The I/O scan set feature allows the scanning of I/O points to be more closely scheduled with its use in user logic programs.

I/O Scan sets that are not scanned every sweep are not guaranteed to be scanned in the same sweep in the Primary and Secondary CPUs. For example, if the Primary and Secondary CPUs each have a scan set that is scanned every other sweep (that is, `PERIOD=2`), the Primary CPU might scan its scan set in one sweep and the Secondary CPU scan its scan set in the next.

Use of non-default scan sets can cause variance in the time the units get to the rendezvous points. This should be considered when determining the Fail Wait time.

## ***STOP to RUN Mode Transition***

A resynchronization will occur at all *STOP* to *RUN* mode transitions. The time to perform this resynchronization may be larger than *STOP* to *RUN* transitions on non-redundancy CPUs. The *STOP* to *RUN* mode transition has two separate paths.

1. If the unit performing the transition is doing so alone or both units are transitioning to Run at the same time, a normal *STOP* to *RUN* mode transition is performed (clear non-retentive memory and initialize #FST\_SCN and #FST\_EXE).
2. If the other unit is active when this unit performs a *STOP* to *RUN* mode transition, non-retentive references will be cleared followed by a resynchronization with the active unit.

## ***Genius Bus Controller Switching***

Genius Bus Controllers stop sending outputs to Genius devices when no output data has been received from the PLC CPU for a period equal to two times the configured watchdog timeout.

If the CPU in the primary unit becomes inoperative in an uncontrolled fashion (for example, because of a power failure), the Genius Bus Controllers detect this within twice the watchdog setting, and stop sending outputs to the Genius devices. After three Genius I/O bus scans of not receiving data from the Genius Bus Controllers at Serial Bus Address 31, the Genius devices start driving data from Serial Bus Address 30 (the secondary unit) if available.

For example, if the system has a 200ms watchdog timeout and 5ms Genius bus scan time, and the primary unit main rack loses power, the Genius Bus Controllers in expansion racks will wait 400ms and then stop updating outputs on Genius devices. After 15ms, the devices will begin driving outputs based on data from the secondary unit. Note that any Genius Bus Controllers in the main rack would stop driving outputs immediately since they would also lose power. Genius devices on these buses would begin driving data from the secondary unit within 15ms.

**Note:** For fastest switching, all Genius Bus Controllers in the Hot Standby CPU Redundancy system should be installed in the main rack. This causes the Genius Bus Controllers to lose power at the same time that the CPU loses power. This, in turn, allows the secondary unit to gain full control of the I/O as soon as possible.

For single bus Genius networks, if outputs are not available on Serial Bus Address 30 or 31, the devices' outputs revert to default or hold last state (as configured).

For dual bus networks, if outputs are not available on Serial Bus Address 30 or 31, then the BSM will switch to the other bus. If outputs are not available on either bus, then the block's outputs revert to default or hold last state (as configured).

## ***Redundant IP Addresses***

Each unit contains at least one Ethernet interface that is assigned a direct IP address used to directly access the specific PLC. A third, redundant, IP address can be assigned to the pair of Ethernet interfaces in both the primary and secondary PLC units. The redundant IP address is active on the Ethernet interface in only one of the PLC units at a time, the active PLC. All data sent to the redundant IP address (including EGD produced to the redundant IP address) is handled by the active PLC. When active, the Ethernet interface always initiates communications using the redundant IP address, when the PLC is in the Backup state, all communications are initiated through the direct IP address.

You can have up to four Ethernet interfaces in each rack, including the CPU's embedded Ethernet interface. Each Ethernet interface can be set up as part of a pair for the purposes of redundant IP. (You can also include Ethernet interfaces in the unit that are not part of a redundant IP pair.)

Immediately after configuration, neither Ethernet interface responds to the redundant IP address. When notified by the CPU that the unit has become active, the Ethernet interface determines whether the redundant IP address is in use on the network. If the address is not in use on the network, the Ethernet interface activates the redundant IP address and sends out an address resolution protocol (ARP) message to force all other Ethernet devices on the network to update their ARP cache. This ARP message is sent so that communications to redundant IP address will be directed to the newly active unit. At this point the Ethernet interface responds to both the redundant IP address and its direct IP address. When commanded to begin EGD production by the CPU, the Ethernet interface in the active unit verifies that it has successfully obtained the redundant IP address. EGD production does not begin until the Ethernet interface obtains the redundant IP address.

If the redundant IP address is in use by another device on the Ethernet network, the Ethernet interface periodically attempts to verify that the address is not in use. The Ethernet interface continues to attempt the redundant IP address verification until it determines the redundant IP address is no longer in use on the network or until the Ethernet interface transitions to Backup due to either a notification from the CPU that the unit has become the backup unit or a failure detection that results in the Ethernet interface transitioning to Backup. This means that if the all of the redundancy links between the two units fails and the units become non-synchronized active, both units will attempt to use the redundant IP address, but only one will succeed. If one of the two units was already active and responding to the redundant IP address, it will continue to do so; the unit that was backup will not be able to activate the redundant IP address.

The Ethernet interface monitors the status of the CPU. If the Ethernet interface determines that it can no longer communicate with the CPU, it deactivates the redundant IP address. The Ethernet interface also deactivates the redundant IP address when notified by CPU that the active unit has transitioned to Backup. When the Ethernet interface deactivates the redundant IP address, it transitions to the Backup state. In the Backup state, the Ethernet interface no longer responds to the redundant IP address, but forwards any packets received by the interface destined for the redundant IP to the Ethernet interface in the active PLC. If the Backup unit continues to receive packets destined for the redundant IP address, it will send additional ARP messages on behalf of the active unit and after a number of time periods, it will log an exception that will be recorded in the PLC CPU fault table as a LAN System Software Fault.

Additional details on the operation of the Ethernet Interface, can be found in *TCP/IP Ethernet Communications for PACSystems*, GFK-2224

---

## *Ethernet Global Data in a Redundancy CPU*

### **Ethernet Global Data Production**

In a redundancy system, only the active unit produces EGD exchanges. This reduces the amount of traffic on the Ethernet network and simplifies the handling of the exchanges by the consumer. In particular, the consumer is able to consume exchanges from the redundant system in the same way it consumes exchanges from non-redundant systems.

When a unit ceases to be the active unit, it stops producing exchanges. If outputs are disabled on the active unit, neither unit produces EGD.

When a given Ethernet Interface is configured to produce EGD, you are required to configure a redundant IP address for that Ethernet network. (This guarantees that a newly active Ethernet interface arbitrates for the redundant IP address and delays EGD production accordingly.) If both redundant units become non-synchronized active units (this can occur at the point where no redundancy links are functioning at all), for each redundant pair, only the Ethernet Interface that owns the redundant IP address will produce exchanges.

The Producer ID as well as all production exchanges should be configured identically for both units. This allows the consumer to continue consuming exchanges from the redundant system when the backup unit becomes active.

### **Ethernet Global Data Consumption**

Both the active and backup units consume EGD exchanges in RUN mode, regardless of whether or not the units are synchronized.

It is recommended that all consumption exchanges be configured identically for both units. In addition, these exchanges must be configured as multicast or directed to the Redundant IP address.

The consumption of multicast exchanges occurs independently on the two units. The Ethernet modules obtain a copy of multicast exchanges at the same time, but reading of that exchange in the two CPUs may be phased by one sweep. This can result in the two units seeing different values for the same exchange in a given sweep. Only the active unit consumes exchanges directed to the Redundant IP address.

If data from the exchanges must be seen identically on the two units, the reference data for the exchanges can be transferred from the active unit to the backup unit during the input data transfer. That transfer occurs shortly after the EGD consumption portion of the CPU sweep. Exchange variables transferred must be placed into %I or %AI memory to participate in the input data transfer.

# Chapter 5

## *Fault Detection*

---

---

This chapter describes how faults are handled in a Redundancy system.

- Fault Detection
- PLC Fault Table Messages for Redundancy
- Fault Response
- Redundancy Link Failures
- Fault Actions in a CPU Redundancy System
- Online Repair

### ***Fault Detection***

The detection of faults and failures falls into three basic categories:

1. Faults and failures that are detected immediately
2. Faults and failures that are detected as soon as possible, but not necessarily within the current sweep
3. Faults and failures that are detected in the background

Faults and failures that are detected immediately are those that are identified within the current sweep. These faults include I/O data corruption, single and multiple bit memory failures, power supply failures, processor failures, and VME transfer failures.

Faults and failures that are detected as soon as possible, but not necessarily within the current sweep, include a group of faults that are not detected by the CPU itself. These faults are typically detected within one second. Genius faults (circuit faults, loss of device, and so forth) fall into this category.

During the background window, additional memory tests are continuously performed. These tests can also detect single and multiple bit memory failures.

## PLC Fault Table Messages for Redundancy

The following table lists messages, descriptions, and corrective actions for error codes associated with the redundancy fault group. These error codes can be viewed in the Fault Tables provided by CIMPLICITY Machine Edition. The entire fault data (including these error codes) can also be accessed using SVC\_REQ 15 and 20.

### Redundancy Fault Group (138)

<b>Error Code</b>	<b>Message</b>	<b>Fault Description</b>	<b>Corrective Action</b>
1	Primary unit is active and secondary unit is backup.	The primary and secondary units have switched roles, the secondary transitioned to Run after the primary, or both units transitioned to Run at the same time.	None required.
2	Secondary unit is active and primary unit is backup.	The secondary and primary units have switched roles, or the primary transitioned to Run after the secondary.	None required.
3	Primary unit is active; no backup unit available.	The primary unit has transitioned to Run mode or secondary unit was put into Stop mode. The primary unit is running without a backup.	To have a synchronized system, the secondary unit <b>MUST</b> be placed in RUN mode with a compatible configuration.
4	Secondary unit is active; no backup unit available.	The secondary unit has transitioned to RUN mode or primary unit was put into Stop mode. The secondary unit is running without a backup.	To have a synchronized system, the primary unit <b>MUST</b> be placed in RUN mode with a compatible configuration.
5	Primary unit has failed; secondary unit is active w/o backup.	The primary unit has recorded a fatal fault or the secondary has lost communications with the primary. The secondary unit is running without a backup.	If primary unit has also logged the fault "Secondary Unit Has Failed: Primary Unit is Active w/o Backup", then communications is broken between the two units and must be repaired. If a fatal fault has been logged in the primary unit, the indicated fault must be repaired. Power may have to be cycled on one of the units in order to re-establish communications and return to a synchronized system.
6	Secondary unit has failed; primary unit is active w/o backup.	The secondary unit has recorded a fatal fault, or the primary unit has lost communications with the secondary. The primary unit is running without a backup.	If secondary unit has also logged the fault "Primary Unit Has Failed: Secondary Unit is Active w/o Backup", then communications has been broken between the two units and must be repaired. If a fatal fault has been logged in the secondary unit, the indicated fault must be repaired. Power may have to be cycled on one of the units in order to re-establish communications and return to a synchronized system.
8	Unable to Switch Redundancy Roles	An attempt to switch redundancy roles was made when it was not possible to perform the switch.	None required.
9	Primary and secondary units are Incompatible	This unit could not be placed into RUN mode because the configurations were	Correct the configurations so that the CPUs have compatible transfer lists and the same point faults enabled

<b>Error Code</b>	<b>Message</b>	<b>Fault Description</b>	<b>Corrective Action</b>
		not compatible.	setting.
10	CPU to CPU communications terminated	Synchronization protocol has been violated.	Contact GE Fanuc technical support. If the fault is accompanied by a Loss of Module fault, see corrective action for "Loss of Module" fault. The link can be restored to service by power cycling either unit or storing configuration to either unit.
11	Redundant Link has timed out	The CPU has timed out while waiting on communications from the other unit.	Contact GE Fanuc technical support. The link can be restored to service by power cycling either unit or storing configuration to either unit.
12	Units Are Not Fully Synchronized	Due to actions taken by the user, the two units in a CPU redundant system are not fully synchronized. This means the backup unit is not executing with the same inputs and/or outputs as the active unit while the units are synchronized due to data transfers being disabled.	Disable the logic that executes SVC_REQ 43.
14	Redundant link communication failure	Communications with the other CPU over this link has failed.	If the other unit failed or lost power, power cycle it. Verify one CPU is configured for primary and the other for secondary. Check the cable connections between the two RMX modules. If the fault is accompanied by a Loss of Module fault, see corrective action for "Loss of Module" fault. Otherwise, contact GE Fanuc technical support.
15	Fail Wait time exceeded	The other CPU failed to rendezvous at a synchronization point within the Fail Wait time.	Increase the configured Fail Wait time.

## Other Fault Groups

The following table lists messages, descriptions, and corrective actions for error codes associated with redundancy in other fault groups.

<b>Group</b>	<b>Error Code</b>	<b>Message</b>	<b>Fault Description</b>	<b>Corrective Action</b>
Loss of Option Module (4)	various	Loss of or missing option module  or Redundant link hard failure occurred	The module is missing or the CPU has determined that the module has failed.	Install the missing module or correct the configuration. Otherwise, replace the module and contact GE Fanuc technical support.
I/O Bus Fault (9)	none	SBA conflict.	The bus controller has detected that another device on the Genius network is already using the same serial bus address.	Verify that one CPU is configured for primary and one for secondary.  Correct the configuration of the Genius devices.
PLC Software (135)	148	Units contain mismatched firmware; update recommended.	The firmware in the redundant CPUs has different revision levels. Having different revisions of firmware in the CPUs is intended for short-term synchronization only as some change in the behavior of the system may be experienced when mixing revisions.	Upgrade the CPUs so that they have the same revision of firmware according to the firmware upgrade procedure.
Configuration Mismatch (11)	75	ECC jumper should be enabled, but is disabled	When redundancy firmware (e.g. CRE020) is installed, the ECC jumper must be in the enabled position.	Set the ECC jumper to the enabled position (jumper on both pins). See the instructions provided with the firmware upgrade kit.
Recoverable Local Memory Error (26)	1	Recoverable local memory error	A single-bit error was encountered and corrected. %SA00006 is set.	The CPU may need to be replaced. Contact GE Fanuc technical support.
CPU Hardware (13)	169	Fatal local memory error	Multiple bit ECC error.	Replace the CPU and contact GE Fanuc technical support.

---

## *Fault Response*

The Hot Standby CPU Redundancy system detects and reports failures of all critical components so that appropriate control actions may be taken. All components that acquire or distribute I/O data or that are involved in execution of the control logic solution are considered critical components.

A FATAL fault in the active unit causes a switch of control to the backup unit. A DIAGNOSTIC fault allows the currently active system to continue operating as the active system.

Faults within the unit may be such that:

1. The CPU has a controlled shutdown,
2. The CPU has an uncontrolled shutdown, or
3. The CPU continues to operate.

If the CPU detects an internal fault and has a controlled shutdown, it logs a fault, goes to Stop/Fault mode, and notifies the other CPU. If the fault was detected on the active unit, the switchover does not normally occur until the next sweep. The exception is when the active unit detects a fatal fault during the input scan. In that case, the two units switch roles just before performing the input data transfer.

If the CPU has an uncontrolled shutdown, the CPU logs a fault if it can and proceeds as described above. When the backup CPU detects that the active CPU has failed (either by receiving notification, by detecting that both redundancy links have failed, or by detecting failure of the active CPU to rendezvous at the next synchronization point within the Fail Wait time) it becomes an unsynchronized active unit.

If the two CPUs lose synchronization for other reasons (due to Fail Wait time set too short or failure of both redundancy links), both units log faults and proceed as non-synchronized active units. In this case both units attempt to control the process independently. The redundant Genius outputs will prefer the output values sent by the active unit.

## ***Redundancy Link Failures***

There are distinct differences between losing a redundancy link and faulting an RMX module.

### **Redundancy Memory Xchange Module Hardware Failure**

Failures such as parity errors and VME bus errors are considered hardware failures of the RMX module. The following actions are taken when such an error is detected:

- Either a Loss of or Missing Option Module or a Redundant Link Hard Failure Occurred fault is logged in the PLC Fault Table
- A Redundant Link Communications Failure fault is logged in both units.
- All LEDs on the RMX module are turned OFF.
- The fault locating references that correspond to the module are set (i.e. the SLOT\_00XX fault contact is set, where XX is the slot number for the RMX module).
- The corresponding redundancy link is no longer used. If the other link is still operating, that link is used for all further data transfer, and the units can remain in synchronization. If the other redundancy link is not available and either unit is in Run mode, that unit operates as a non-synchronized active unit.

Power must be cycled on the rack to restore a faulted RMX module to service.

### **Redundancy Link Communications Failures**

The following errors are reported as failures of the redundancy link:

- The other unit has lost power or failed such that it can no longer communicate.
- One or both cables between the two RMX modules have failed or are disconnected.
- A network error was detected on the fiber optic link that connects the two RMX modules. (This includes data checks on mismatches, protocol errors, and rogue packets.)
- Failure of the other CPU to rendezvous at the next synchronization point within the Fail Wait time.

The following actions are taken when a redundancy link communications failure occurs:

1. Either a Redundant Link Communications Failure or Fail Wait Time Exceeded fault is logged in the PLC Fault Table of both units.
2. The LINK OK LEDs on both RMX modules are turned off.
3. The fault locating references that correspond to the module are set (i.e. the SLOT\_00XX fault contact is set, where XX is the slot number for the RMX module).
4. The corresponding redundancy link is no longer used. If the other link is still operating, that link is used for all further data transfer, and the units can remain in synchronization. If the other redundancy link is not available and either unit is in Run mode, that unit operates as a non-synchronized active unit.

If the RMX modules' OK LEDs are still ON, the link can be restored to service by power cycling either unit or storing a hardware configuration to either unit. If either OK LED is OFF, power must be cycled on the rack to restore that RMX module to service.

## *Fault Actions in a CPU Redundancy System*

Fault actions in the Hot Standby CPU Redundancy System are handled differently than fault actions in a non-redundant system. Whenever the units are synchronized, the types of faults that are considered to be FATAL (i.e., cause the CPU to stop) are not configurable. The following types of faults are considered FATAL when the units are synchronized:

- any fault that causes loss of control of I/O
- any fault that degrades performance

**Note:** In a CPU redundancy system a *Fatal* fault from a Genius Bus Controller causes a synchronized unit to transition to *STOP/FAULT* mode. All *Diagnostic* faults allow the CPU to remain in Run mode.

## Configuration of Fault Actions

You can configure whether certain faults are considered fatal when the CPUs are not synchronized.

The following should be considered when configuring the fault actions for a redundancy CPU. For a given fault that is fatal for the synchronized case, if you set the non-synchronized fault action to be diagnostic, there is a chance that a less healthy unit could remain the active unit even after a more healthy backup unit is placed in Run mode. For example, if you were to configure "Loss of or Missing Rack" failures as diagnostic, the following sequence of events could occur:

1. If an expansion rack fails when the units are synchronized, the unit with the rack failure will transition to STOP/FAULT mode and the other unit will become a non-synchronized active unit.
2. If an expansion rack fails in the non-synchronized active unit, a diagnostic fault will be logged but the unit will stay in RUN mode and continue to control the process.
3. If the first unit is repaired and then transitions to Run, the second unit with the failed expansion rack will stay in RUN mode and will remain in control of the process.

To prevent this situation, you may want to include logic to shut down the less healthy unit or request a role switch.

Also, a unit with the fault actions set to diagnostic may be placed in RUN mode and become the active unit even though it may have a diagnostic fault, which would be logged as fatal in a synchronized system.

For example, if an expansion rack fails while in STOP mode or while transitioning to RUN mode, a diagnostic fault is logged. However, the unit will still transition to RUN. In addition, if you have programmed a Preferred Master algorithm, this unit will become the active unit. To prevent this situation, you may want to include logic to shut down the less healthy unit or modify the role switch logic.

## Configurable Fault Groups

The table below shows the configurable faults and their fault actions. There are three fault actions: *Fatal*, *Diagnostic*, and *Conditionally Fatal*. Fatal always stops the PLC, Diagnostic

never stops the PLC, and Conditionally Fatal stops the PLC depending on other information in the fault.

<b>Fault Group</b>	<b>Table Type</b>	<b>Description</b>	<b>Non-Synchronized Fault Action</b>		<b>Synchronized Fault Action (fixed)</b>
			<b>Default</b>	<b>Configurable</b>	
LOSS_RACK (1)	PLC	Loss of or Missing Rack	Diagnostic	Yes	Fatal
LOSS_IOC (2)	I/O	Loss of or Missing I/O Controller	Diagnostic	Yes *	Fatal
LOSS_IO_MOD (3)	I/O	Loss of or Missing I/O Module	Diagnostic	Yes	Diagnostic
LOSS_OTHR_MOD (4)	PLC	Loss of or Missing Option Module	Diagnostic	Yes	Diagnostic
SYS_BUS_ERROR (12)	PLC	System Bus Error	Fatal	Yes	Fatal
IOC_FAULT (9)	I/O	IOC or I/O Bus Fault	Diagnostic	Yes	Conditionally Fatal**
CNFG_MIS_MTCH (11)	Both	System Configuration Mismatch	Fatal	Yes	Diagnostic
IOC_SOFTWR (15)	I/O	IOC Software Failure	Diagnostic	Uses LOSS_IOC setting	Conditionally Fatal**
OVER_TMP (24)	PLC	CPU Over Temperature	Diagnostic	Yes	Fatal
LOC_MEM_ERROR (38)	PLC	Recoverable Local Memory Error	Diagnostic	Yes	Diagnostic

\* Even if the non-synchronized fault action for the LOSS\_IOC fault group is configured as Fatal, the PLC will not go to STOP/FAULT mode unless *both* Genius Bus Controllers of a dual bus pair fail.

\*\* Conditionally Fatal: When the units are synchronized, the two fault groups IOC\_FAULT and IOC\_SOFTWR faults are fatal if the Genius Bus Controller reports the fault as Fatal. When a GBC logs one of these faults, it notifies the PLC whether or not it can continue by placing Fatal or Diagnostic in the fault action of the fault entry.

## Non-Configurable Fault Groups

The table below shows the non-configurable faults and their fault actions. There are two fault actions: *Fatal* and *Diagnostic*. Fatal always stops the PLC and Diagnostic never stops the PLC.

<b>Fault Group</b>	<b>Table Type</b>	<b>Description</b>	<b>Fault Action</b>
SYS_BUS_FAIL	PLC	System bus failure.	Fatal
NO_USER_PRG	PLC	No User's Program on Power-up.	Diagnostic
BAD_USER_RAM	PLC	Corrupted User RAM detected on Power-up.	Fatal
WIND_CMPL_FAIL	PLC	Window Completion Failure in Constant Sweep Mode (i.e., all windows failed to receive their allotted time).	Diagnostic
PASSWD_FAIL	PLC	Password Access Failure.	Diagnostic
NULL_SYS_CNFG	PLC	NULL System Configuration for RUN Mode.	Diagnostic
CPU_SOFTWR	PLC	PLC CPU Software Failure.	Fatal
SEQ_STORE_FAIL	PLC	<i>Communication</i> failure during a store operation by the programmer. This fault results when the start-of-store sequence was received but not an end-of-store sequence.	Fatal
ADD_RCK	PLC	Addition of Extra Rack	Diagnostic
ADD_IOC	I/O	Addition of or Extra IOC	Diagnostic
ADD_IO_MOD	I/O	Addition of or Extra I/O Module	Diagnostic
ADD_OTHR_MOD	PLC	Addition of, Reset of, or Extra Option Module	Diagnostic
IO_MOD_FAULT	I/O	I/O Module Fault	Diagnostic
CPU_HARDWR	PLC	CPU Hardware Failure	Fatal
MOD_HARDWR	PLC	Module Hardware Failure (for example, Serial Port Failure on PCM)	Diagnostic
MOD_OTHR SOFTWR	PLC	Option Module Software Failure	Diagnostic
PRG_BLK_CHKSUM	PLC	Program Block Checksum Mismatch	Fatal
LOW_BATTERY	PLC	Low Battery in the System	Diagnostic
CNST_SW_EXCD	PLC	Constant Sweep Exceeded	Diagnostic
PLC_FTBL_FULL	PLC	PLC System Fault Table Full	Diagnostic
IO_FTBL_FULL	PLC	I/O Fault Table Full	Diagnostic
APPLICATION_FLT	PLC	User Application Fault	Diagnostic

## Fatal Faults on Both Units in the Same Sweep

It is very unlikely that a fatal fault would occur on both units in the same sweep. If that should happen, however, the first CPU to detect a fatal fault will use the synchronized fault action table. The other CPU will use the non-synchronized fault action table. This allows one of the units to stay in Run mode when the synchronized fault action is Fatal and the non-synchronized fault action is diagnostic.

## ***Online Repair***

With a Hot Standby CPU Redundancy system, most system component failures can be repaired by replacing the failed component while the system is online.

### **On-Line Repair Recommendations**

To replace a component online, it is strongly recommended that you follow this procedure:

1. Make sure the unit to be repaired is the backup unit. (The LOCAL ACTIVE LED should be OFF and the REMOTE ACTIVE LED should be ON. You can also confirm this by viewing the Redundancy tab of the programmer's online status dialog box.) If unit to be repaired is already in Stop mode, skip this step. If the unit to be repaired is active, activate the Role Switch on the RMX module.
2. Power-off the unit to be repaired.
3. Replace the defective component.
4. On the CPU of the repaired unit, place the Run/Stop switch in the Stop position.
5. Power on the repaired unit.
6. After several seconds, verify that the LINK OK LEDs are ON for all RMX modules in both units. If the LINK OK LEDs are not on, see the PLC Fault Table.
7. If the repaired CPU is in Stop/Fault mode, verify that there are no unexpected faults and then clear the Fault Tables.
8. Place the repaired unit into RUN mode by putting the Run/Stop switch in the Run position.

## **Online Repair of the Genius Bus**

### **Single Bus Networks**

The Genius bus of a single bus network can be repaired without disturbing power to either unit. However, repairing the bus without taking the entire Hot Standby CPU Redundancy system offline is not recommended because all devices on that bus will be disconnected from the controllers while the bus is being repaired.

### **Dual Bus Networks**

The Genius bus of a dual bus network can be repaired without disturbing power to either unit. It is recommended that you disconnect the failed bus from the GBCs before you attempt to repair it.

# Chapter 6

## *Converting a Series 90-70 Redundancy System to PACSystems*

---

---

Converting a Series 90-70 redundancy target to PACSystems is very similar to converting a non-redundant target. This chapter describes conversion issues that apply only to redundancy systems. Before converting your application, you should review “Converting Series 90-70 Applications to PACSystems” in the *CPU Reference Manual*, GFK-2222.

### Warning

**There may be execution differences when converting an application from a Series 90-70 target to a PACSystems RX7i target. It is the application developer's responsibility to validate and test the application execution prior to deployment into a production environment.**

The programming software automatically makes the following changes to the configuration during the conversion:

- The redundancy CPUs from the 90-70 rack system are converted to CRE020 CPUs. The Redundancy tab parameters are copied without any changes.
- The Series 90-70 RCM is replaced with two RMX modules.
- The Control Strategy setting in the CPU (GHS or GDB) is changed to HSB.

### *Control Strategy Conversion*

PACSystems supports only the HSB control strategy, which is equivalent to the GDB control strategy in the Series 90-70 PLC. The GHS configuration option is not supported by PACSystems.

With the HSB control strategy, all redundant Genius outputs must be included in the Output Transfer List. For details, refer to “Transfer List” in chapter 3.

If your 90-70 target used the GHS control strategy, you may need to adjust the %Q and %AQ ranges in the Output Transfer list so that they include all redundant Genius outputs. In addition, if preferred master is desired, Ladder Logic application programming is required (see “Logic for Implementing Preferred Master” in chapter 4).

Check your program logic for the use fault locating references that correspond to the remote RCM (rack 7). Adjust them to refer to the local RMX modules.

---

## *Applications with a Programmable Coprocessor Module*

If your 90-70 application includes a Programmable Coprocessor Module (IC697PCM711), you may need to adjust the application running in the PCM to make it compatible with the PACSystems version of CPU redundancy. Specifically, when power is applied to the Rx7i rack, the Rx7i Redundancy CPU can take a longer time to respond to the first communication request made by the PCM. To account for this delay, you could adjust your PCM application so that it retries the first communication requests for approximately 60 seconds before declaring an error.

**#**

#OVR\_PRE, 2-2, 4-5

**%**

%S references, 4-5  
#OVR\_PRE, 2-2

**A**

Active unit  
defined, 1-2

**B**

Background Window time  
different for redundancy CPUs, 2-3  
Backup Unit  
defined, 1-2  
switching control to, 4-14  
commanding from program, 4-14  
switching times, 4-14  
validating the input scan, 4-13  
validating the logic solution, 4-13  
Bus Controller, Genius  
configuring, 3-12  
description, 2-4  
installation requirements, 2-4  
installing dual GBCs at same end of bus, 2-8  
switching, 4-18

**C**

Communications  
terminating, 5-6  
Configurable fault groups, 5-7  
Configuration, 3-4  
storing (downloading), 3-13  
Constant Sweep mode, 3-5  
Contacts, timed, 4-17  
Control strategy, 1-3  
CPU parameters, 3-4  
Faults, 3-6  
Redundancy, 3-7  
Settings, 3-4  
Transfer List, 3-8  
CPU Redundancy  
defined, 1-2  
Critical component  
defined, 1-2

**D**

Data transfer  
from backup to active unit, 4-9  
time, 4-8  
Data Transfer, 4-7  
inputs, 4-7  
outputs, 4-7  
Disable data transfer copy in backup unit,  
4-11  
Downloading configuration, 3-13  
Dual Bus  
defined, 1-2  
Duplex Genius output mode, 2-8

**E**

Error checking and correction (ECC), 2-3,  
4-16  
fault configuration, 3-6  
Ethernet controller  
configuring communications window, 3-5  
Ethernet global data  
consumption, 4-21  
in a redundancy system, 4-21  
production, 4-21  
redundant IP addresses, 4-19  
Ethernet Interface  
parameters, 3-11

**F**

Fail Wait time, 3-7, 4-6  
Fault actions, 5-7  
configuration, 5-7  
configured differently for redundancy CPUs,  
2-3  
Fault detection, 5-1  
Fault groups  
configurable, 5-7  
non configurable, 5-9  
Fault messages for redundancy, 5-2  
Fault response, 5-5

**G**

Genius blocks  
configuring, 3-12  
installing on same end of bus, 2-8

**H**

Hot Standby  
defined, 1-2  
Hot Standby CPU redundancy, 1-1  
features, 1-3

HSB control strategy, 4-4  
HSB operation, 1-4

## I

I/O scan sets, 4-17  
I/O systems  
    description, 2-4  
IEC Transitionals, 4-7  
Input data transfer, 4-7  
Interrupts  
    cannot be enabled in HSB system, 3-12  
    not available with Redundancy CPUs, 2-2

## L

LEDs, 2-4  
Links  
    losing, 5-6  
Local I/O, 2-9

## M

Multiple I/O scan sets, 4-17

## N

Non configurable fault groups, 5-9  
Non redundant operation, 2-3  
    configuring, 3-13

## O

Online programming, 1-5  
Online repair, 1-5  
    description, 5-10  
Output control, 1-4  
Output data transfer, 4-7

## P

Parameters, 3-4  
PID function blocks, 4-17  
Powerup, 4-2  
    sequence for full redundancy at powerup, 4-2  
Powerup sequence, 4-2  
Preferred master, 4-15  
Primary unit  
    defined, 1-2  
    powerup sequence, 4-2  
Programmable Coprocessor Module (PCM), 6-2  
Programming

online, 1-5

## R

Racks  
    for redundancy systems, 2-1  
    VME racks not supported, 2-1  
Redundancy  
    configuration wizards, 3-2  
    defined, 1-2  
    parameters  
        CPU, 3-7  
Redundancy CPUs  
    description, 2-2  
    differences from other CPUs, 2-2  
    features, 1-3  
    powerup, 4-2  
Redundancy Memory Xchange (RMX)  
    module  
    description, 2-3  
    faulting, 5-6  
    parameters, 3-10  
Redundant IP addresses, 4-19  
Repair  
    online, 1-5  
Resynchronization, 4-3  
Run/Disabled mode, 4-16  
    different for redundancy CPUs, 2-3

## S

Scan sets  
    multiple, 4-17  
Scan synchronization, 4-6  
Secondary unit  
    defined, 1-2  
    powerup sequence, 4-2  
Service requests  
    26, Implementing preferred master, 4-15  
    26, Role switch from program, 4-14  
    27, Write to reverse transfer area, 4-9  
    28, Read from reverse transfer area, 4-9  
    43, Backup qualification, 4-13  
    43, Disable data transfer copy in backup unit, 4-11  
Stop I/O Scan mode  
    not available with Redundancy CPUs, 2-2  
Stop to Run mode transition, 4-18  
    different for redundancy CPUs, 2-3  
Storing configuration, 3-13  
Sweep time synchronization, 4-7  
Synchronization  
    scan, 4-6  
Synchronized  
    defined, 1-2  
System Communications Window, 3-5

## **T**

- Timed contacts, 4-17
- Timer function blocks, 4-17
- Transfer List parameters
  - CPU, 3-8
- Transfer time, 4-8
- Transition contacts and coils, 4-7

## **W**

- Watchdog timer
  - Genius bus, 2-5, 2-7
- Wizards, 3-2